LANTRONIX®

SecureLinx™ SLP Remote Power Manager User Guide

Part Number 900-371
Revision C January 2009

Copyright & Trademark

Ethernet is a trademark of XEROX Corporation. UNIX is a registered trademark of The Open Group. Windows 95, Windows 98, Windows 2000, and Windows NT are trademarks of Microsoft Corp. Netscape is a trademark of Netscape Communications Corporation.

Contacts

Lantronix Corporate Headquarters
15353 Barranca Parkway
Irvine, CA 92618, USA
Phone: 949-453-3990
Fax: 949-453-3995

Technical Support
Phone: 800-422-7044 or 949-453-7198
Fax: 949-450-7226
Online: www.lantronix.com/support

Sales Offices
For a current list of our domestic and international sales offices, go to the Lantronix web site at www.lantronix.com/about/contact.

Disclaimer & Revisions

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference in which case the user will be required to correct the interference at his or her own expense.

Instructions

This symbol is intended to alert the user to the presence of important operating and maintenance (servicing) instructions in the literature accompanying the appliance.

Dangerous Voltage

This symbol is intended to alert the user to the presence of un-insulated dangerous voltage within the product's enclosure that may be of sufficient magnitude to constitute a risk of electric shock to persons.

Protective Grounding Terminal

This symbol indicates a terminal that must be connected to earth ground prior to making any other connections to the equipment.

Life-Support Policy

As a general policy, Lantronix does not recommend the use of any of its products in the following situations:

- Life-support applications where failure or malfunction of the Lantronix product can be reasonably expected to cause failure of the life-support device or to significantly affect its safety or effectiveness.
- Direct patient care.

Lantronix will not knowingly sell its products for use in such applications unless it receives in writing assurances satisfactory to Lantronix that:

- The risks of injury or damage have been minimized,
- The customer assumes all such risks, and
- The liability of Lantronix is adequately protected under the circumstances.

The term life-support device includes but is not limited to neonatal oxygen analyzers, nerve stimulators (whether used for anesthesia, pain relief or other purposes), auto-transfusion devices, blood pumps, defibrillators, arrhythmia detectors and alarms, pacemakers, hemodialysis systems, peritoneal dialysis systems, neonatal ventilator incubators, ventilators (for adults or infants), anesthesia ventilators, infusion pumps, and any other devices designated as “critical” by the U.S. FDA.

The information in this guide may change without notice. The manufacturer assumes no responsibility for any errors that may appear in this guide.

For the latest revision of this product document, please check our online documentation at www.lantronix.com/support/documentation.html.

Date	Rev.	Comments
12/2004	A	Initial Document
5/2006	B	Part number changes related to RoHS.
1/2009	C	Updated entire document, added RoHS changes.

Contents

List of Figures

List of Tables

1: Introduction

The Lantronix SLP Remote Power Manager family of products provides easy, practical, and secure solutions for power distribution, power management and load-measurement for remote equipment and branch AC circuits.

The SLP Remote Power Manager supports the elimination of unnecessary trips to remote locations by allowing remote control of the power on/off status for distant critical equipment, minimizing the impact of locked-up devices on mission-critical systems.

Features and Benefits

SLP models are available in 8-outlet and 16-outlet configurations for 100-120VAC and 208-240VAC up to 16A. Expansion models are available in 8-outlet and 16-outlet configurations for 100-120VAC and 208-240VAC up to 16A. See *Models* on page 101.

Communication Access Modes

All models are equipped standard with a RS-232 (serial) port and a 10/100 Base-T Ethernet port for Telnet, Secure Shell (SSH), and web browser access.

Power Distribution

Up to 16A/24A of AC power (dependant on model) can be distributed across up to sixteen attached devices. See *Models* on page 101 for available models.

Remote Power Management

Remote control of power outlets allows individual on/off and reboot control of up to 16 devices or up to 32 devices with the addition on an expansion unit.

Load and Environment Measurement

Load measurement eliminates guesswork by supplying the cumulative operating load in amperes. This allows on-site technicians to maximize the equipment installed and operated on a circuit without concern. Use of the circuit is maximized, while effectively allowing a 10% to 20% safety margin. Remote users also may access this information at any time from the command line or web browser interface.

Optionally, temperature and humidity sensors allow monitoring of key environmental conditions at remote facilities.

Power-up Sequencing

When powered on, each of the power outlets power sequentially with a two-second delay between each outlet. Power sequencing staggers the individual loads, eliminating the potential of a blown fuse or circuit breaker due to excessive in-rush current and allows circuit support for operating load capacities of 80% to 90%.

Outlet Grouping

For operations across multiple attached devices or devices with multiple or redundant power supplies, include outlets in one or more named groups of outlets. This allows changes to all outlets in the named group with a single command sequence.

Security

Units ship with one predefined administrative user account. The administrator can create up to 128 user accounts, with individualized access to outlets and commands. All accounts support username and password protection. For configurations requiring multiple fully-privileged users, the administrator can grant administrative privileges to other user accounts in the system.

User Interfaces and LEDs

Two types of user interfaces are available: the web browser and the command line interface. For easy outlet recognition, assign descriptive names to both individual outlets and outlet groups for use in control commands. For the on-site technician, LEDs indicate individual outlet power status and cumulative power load.

Automatic Timeout

For added security, a user session automatically terminates after five minutes of inactivity; if a user is called away unexpectedly, an unprotected channel does not remain open indefinitely.

2: Installation

Prior to installation, refer to the following lists to ensure that you have all the items shipped with the unit as well as all other items required for proper installation.

Standard Accessories

- Mounting bracket hardware:

  Vertical (SLP-V, SLPY* models) – two removable flanges with four M4 screws and two mounting L-brackets with two nut plates and four sets of screws and washers

  Horizontal/Rack (SLP-H, SLPX* models) – two mounting brackets and four screws
- RJ45 to RJ45 serial rollover cable
- RJ45 to DB9F serial port adapter (for connection to standard DB9M DTE serial port)
- Outlet retention clips, one per outlet (208-240V units only)
- Power input retention bracket hardware
- Two removable T-brackets with two 40mm screws
- Additional required Items:

  Phillip screwdriver

  Screws, washers and nuts to attach the SLP to your rack

  Power input cord (purchased separately)

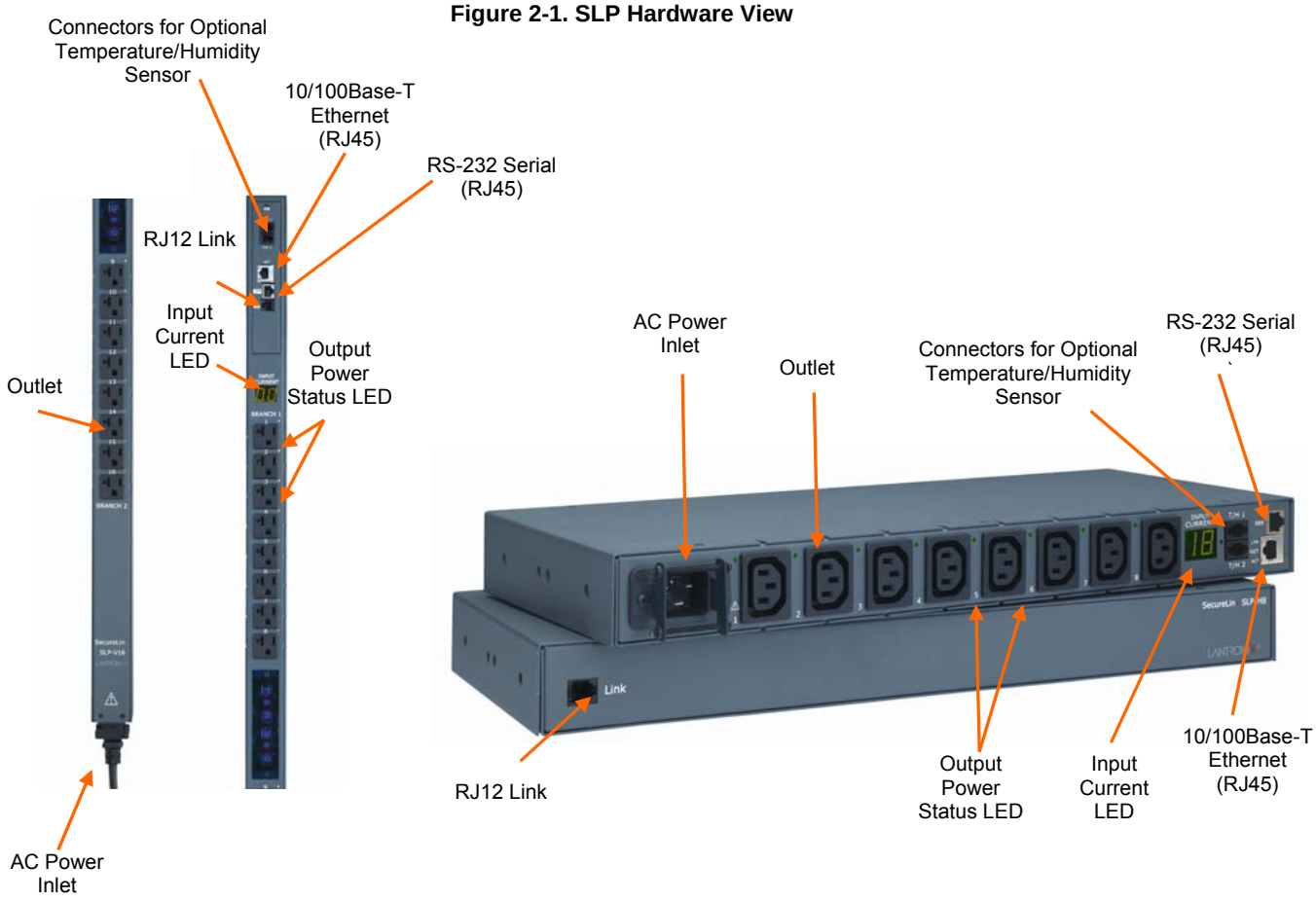
  *SLPY, SLPX includes RJ12 link cable

Equipment Overview

The outlets are labeled 1 through 16. These numbers may be used in commands that require an outlet name. See *Outlet Naming and Grouping* for more information. The power inlet connects to the electrical power source. Figure 2-1 shows the hardware features of the SLP.

Note: *Models SLP-H8 and SLP-V16 are displayed in the following illustration. Other models may have variations.*

Figure 2-1. SLP Hardware View



Safety Precautions

This section contains important safety and regulatory information that should be reviewed before installation. For input and output current ratings, see Power Ratings in *Technical Specifications*.

Only for installation and use in a Service Access Location in accordance with the following installation and use instructions.

This equipment is designed to be installed on a dedicated circuit.

Dedicated circuit must have circuit breaker or fuse protection.
This product has been designed without a master circuit breaker or fuse to avoid becoming a single point of failure. It is the customer's responsibility to provide adequate protection for the dedicated power circuit. Protection of capacity equal to the current rating of the product must be provided and must meet all applicable codes and regulations. In North America, protection must have a 10,000A interrupt capacity.

The plug on the power supply cord shall be installed near the equipment and shall be easily accessible.

Installation Orientation: SLPVxxxx-02 units are design to be installed in vertical orientation.

Always disconnect the power supply cord before opening to avoid electrical shock.

Warning! High leakage current! Earth connection is essential before connecting supply!

Warning: 208-240/230V models only: Outlets are not fused. Outlet circuit protection is provided by the building installation, which shall not exceed 30A branch circuit protection

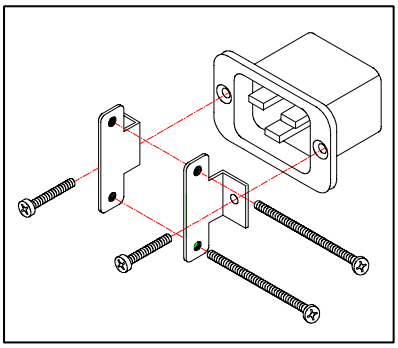
Installing the Power Input Retention Bracket

For models with a total maximum output < 30A, it may be necessary to install the power input retention bracket prior to mounting the unit within a rack.

To install the power input retention bracket:

1. Remove the two screws attaching the IEC 60320 C19 inlet to the enclosure.
2. Assemble and attach the retention bracket to the enclosure as shown:

Figure 2-2. Retention Bracket Assembly



Mounting

Horizontal/Rack

1. Select the appropriate bracket mounting points for proper mounting depth within the rack.
2. Attach the brackets to these mounting points with two screws for each bracket.
3. Install the enclosure into your rack, using the slots in each bracket. The slots allow about ¼ inch of horizontal adaptability to align with the mounting holes of your rack.

Vertical

1. Attach the removable flanges to the mount points on the rear of the enclosure using M4 screws.
2. Attach the mounting L-brackets to the flanges with the supplied screws, washers and nut plates. The slots allow about 1½ inches of vertical adaptability.
3. Attach the top and bottom brackets to your rack.

Connecting to the Power Source

Attach the power cord to the unit before connecting the unit to the power source. Each outlet powers up sequentially, with a two-second delay between each outlet, eliminating a potential blown primary fuse or circuit breaker from excessive in-rush current.

To attach a power cord to the unit:

1. Plug the female end of the power cord firmly into its connector at the base.
2. Use a screwdriver to tighten the two screws on the retention bracket.

To connect to the power source:

1. Plug the male end of the power cord into the AC power source.

Connecting Devices

To avoid the possibility of noise due to arcing:

1. Keep the device's on/off switch in the off position until after it is plugged into the outlet, or log in to the unit and turn the outlets off before connecting the devices
2. Connect devices to the outlets.

   On 230V units, install a retention clip for each outlet; Pull the prongs out slightly and insert them into holes on the sides of the unit, then insert the device's power cord and snap the clip over the cord.

Note: *Even distribution of attached devices is recommended across the available outlets to avoid exceeding the outlet, quad or octet ratings limitations. See Technical Specifications on page 101 more information.*

Note: *The outlet retention clips on the 230V models are designed for use with Lantronix provided cables. The retention clip may not properly fit 3rd party cables.*

Always disconnect the power supply cord before opening to avoid electrical shock.

Connecting to a local Personal Computer (PC)

Serial (RS-232) port

All models are equipped with an RS-232 port (RJ45) for attachment to a PC using the supplied RJ45 to RJ45 serial rollover cable and an RJ45 to DB9F adapter. See *Technical Specifications* on page 103 for more information on the RS-232 serial port. The default values are 9600 baud, 8 data bits, 1 stop bit, no parity (9600 8N1).

Ethernet port

All models are equipped with a 10/100Base-T Ethernet port for attachment to an existing network. This connection allows access via Telnet, Secure Shell (SSH), or web browser.

The following network defaults allow unit configuration out-of-the-box through either Telnet/SSH or via a web browser:

IP address:	192.168.1.254
Subnet Mask:	255.255.255.0
Gateway:	192.168.1.1

The local PC network connection must be configured as Noted below:

Note: *Contact your system administrator for instructions in reconfiguring the network connection. Reconfiguration of your network connection may require a restart to take effect.*

IP address:	192.168.1.x (where x is 2-253)
Subnet Mask:	255.255.255.0

3: Operations

User Interfaces

Two user interfaces are available: the web browser interface accessed via the HTTP/SSL enabled Ethernet connections and the command line for serial and Telnet/SSH connections.

Outlet Naming and Grouping

For commands requiring an outlet name, you may specify it in one of two ways: a predefined absolute name or a descriptive name assigned by an administrator.

Models with a Single Power Infeed

Absolute names are specified by a period (.) followed by a unit letter and outlet number.

Usernames and Passwords

The factory default has one predefined administrative user account (username/password: sysadmin/PASS) and supports a maximum of 128 defined user accounts

Note: *For security purposes, it is recommended that the predefined administrative user account be removed after a new account with administrative rights has been created.*

Only an administrative-level user may perform operations such as creating/removing user accounts and command privileges, changing passwords and displaying outlet and user information. An administrator may also view the status of and control power to all outlets.

The administrator may create additional user accounts and then grant these users the right to view the status of and control power to specific outlets, groups and ports.

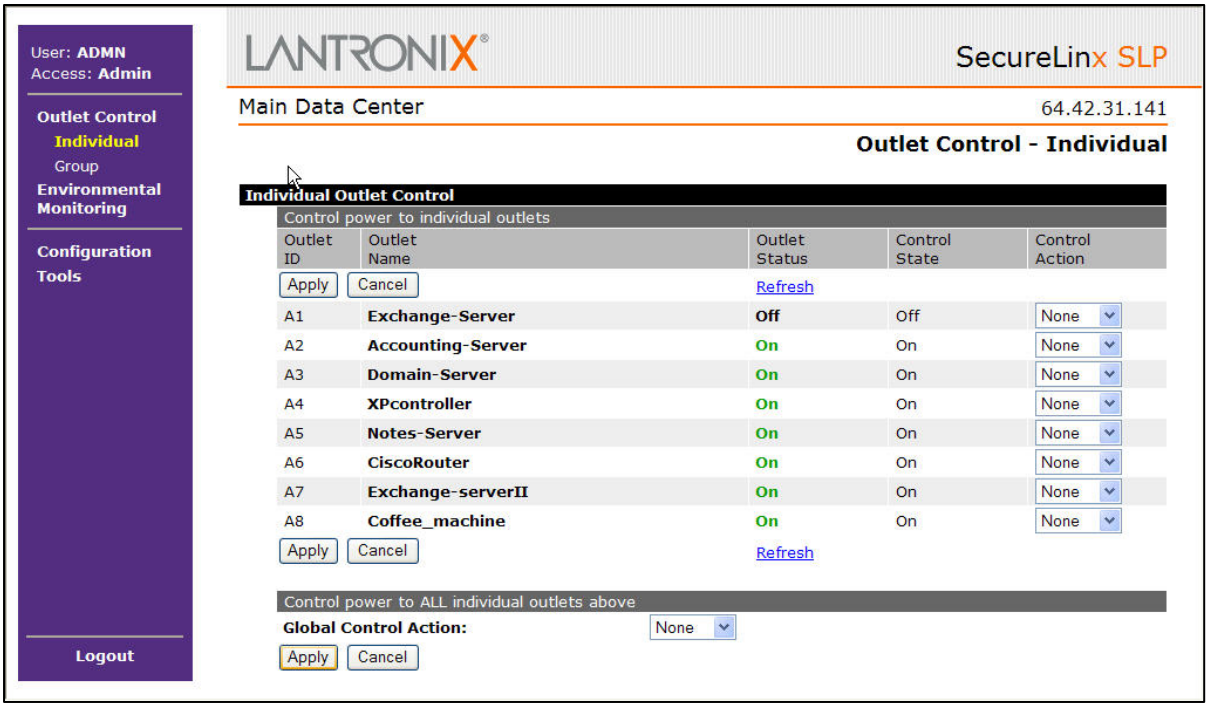
Usernames may contain from 1-16 characters and are not case sensitive; spaces are not allowed. Passwords may contain up to 16 characters, and are case sensitive.

Web Browser Interface

The web browser interface is constructed of three major components: the **System Location** bar, the **User/Navigation** bar and the **Control Screen**. The **System Location** bar displays the location and IP address as well as the current **Control Screen** title. The **User/Navigation** bar displays the current user and privilege level and provides access to all monitoring and control pages. The **Control Screen** is

used to display current data and allow changes to outlet states or system configuration.

Figure 3-1. Web Browser Interface



The following sections describe each interface section/page and their use.

Logging In

Logging in via a web browser requires directing the web client to the configured IP address of the unit.

To log in by web browser:

1. In the login window, enter a valid username and password and press **OK**. (Default username/password:sysadmin/PASS).

   If you enter an invalid username or password, the prompt will repeat again.

   You are given three attempts to enter a valid username and password combination. If all three fail, the session ends and a protected page will be displayed.

Outlet Control

The **Outlet Control** section offers access to the **Individual** and **Group** outlet control pages. From the **Individual** and **Group** pages, the user can review and manipulate power control functions for all outlets and groups assigned to the current user. Both pages include the outlets absolute and descriptive names, the Outlet Status reported to the unit by the outlet, the current Control State being applied by the unit and the outlet load in amperes.

Available outlet and group power states may be set to on, off or reboot; the reboot operation turns the outlet(s) off, delays for a period of 15 seconds and then turns the outlet(s) on.

Individual

The **Individual** outlet control page displays all outlets assigned to the current user. The user may apply on, off or reboot actions to individual, multiple or all accessible outlets.

To apply actions to individual or multiple outlets:

1. In the Individual Outlet Control section, select the desired action from the Control Action drop-down menu for each individual outlet to be changed and press **Apply**.

To apply an action to all outlets:

1. In the Global Control section, select the desired action from the Control Action drop-down menu and press **Apply**.

Group

The **Group** outlet control page displays all groups assigned to the current user as well as the outlets for each group.

To select a group:

1. Select the group name from the drop-down menu and press **Select**. The page will refresh to display all outlets associated to the selected group name.

To apply an action to a group:

Select the desired action from the drop-down menu and press **Apply**.

Table 3-1. Outlet State/Control State Field Values

Outlet State	Control State	Description
On	On	Outlet is on
Off	Off	Outlet is off
Off	Pend On	Outlet is off and about to turn on in response to a sequence timer
Off	Reboot	Outlet is off and a Reboot action has been initiated
On	Idle On	A restart has occurred – Last Control State has been maintained
Off	Idle Off	A restart has occurred – Last Control State has been maintained
On	Wake On	A power-loss has occurred – Wakeup State has been applied
Off	Wake Off	A power-loss has occurred – Wakeup State has been applied
On/Wait	Off	Outlet state in transition – Re-query of outlet status required
Off/Wait	On	Outlet state in transition – Re-query

Outlet State	Control State	Description
		of outlet status required
On/Error	varies	Error State – Outlet should be off but current is sensed at the outlet
Off/Error	varies	Error State – Outlet should be on but no current is sensed at the outlet
Off/Fuse	On	Outlet should be on but a blown fuse has been detected.
No Comm	varies	Communication to the outlet has been lost*

*** Control State will be applied when communication is re-established**

Environmental Monitoring

The **Environmental Monitoring** section offers access to the Input Load page. This section is available to administrative level users and users with Environmental Monitoring view rights.

Input Load

The **Input Load** page displays the absolute and descriptive name and the cumulative input load in amperes of all devices attached to the unit at the time the page was loaded. This page will refresh automatically every 10 seconds.

Sensors

The **Sensors** page displays the temperature/humidity sensor's absolute and descriptive names. The sensor page also displays temperature/humidity sensor readings in degrees Celsius and percent relative humidity. This page will refresh automatically every 10 seconds.

Configuration

The Configuration section offers access to all unit configuration options including System, Network, Telnet/SSH, HTTP/SSL, Serial Port, Outlets, Groups, Users, FTP, SNTP/Syslog,SNMP, LDAP, TACACS+ and Email. This section is available to administrative level users only.

System

The **System** configuration page is used for reference of system information such as Ethernet NIC Serial Number, Ethernet MAC address and system firmware and hardware revisions as well as assignment and maintenance of the system location and unit descriptive names.

For description names, up to 24 alphanumeric and other characters (ASCII 33 to 126 decimal – spaces and colon characters are not allowed) are allowed.

Note: *Spaces may be used for the location description only.*

Creating a descriptive system location name:

1. Enter a descriptive name and press **Apply**.

Configuring the Input Current LED display orientation:

1. Select **Normal** or **Inverted** from the drop-down menu and press **Apply**.

Enabling or disabling strong password requirements:

1. The SLP supports enforcement of strong passwords for enhanced security. When enabled, all new passwords must be a minimum of 8 characters in length with at least one uppercase letter, one lowercase letter, one number and one special character.

2. ***Acceptable strong passwords:***

   n0tOnmyw@tch

   john2STI?

   H3reUgo!

Note: *Strong password requirements also enforce a minimum change of four character positions when defining new strong passwords.*

3. Select **Enabled** or **Disabled** from the Strong Passwords drop-down menu and press **Apply**.

Note: *The strong password requirement is applied against all new passwords.*

Enabling or disabling the external reset button:

1. Select **Enabled** or **Disabled** from the External Reset Button drop-down menu and press **Apply**.

Setting the temperature scale:

Select Celsius **or** Fahrenheit **from the Temperature Scale drop-down menu and press** Apply**.**

Creating a pre-login banner:

1. Click on the **Login Banner** link.

2. On the subsequent **Login Banner** page, enter a pre-login banner and press **Apply**.

Note: *The pre-login banner may be up to 2070 characters in length and is displayed prior to the login prompt. If left blank, no system banner will be displayed prior to login prompt.*

Creating a descriptive unit name:

1. Click on the **Tower Names** link.

2. On the subsequent page, enter a descriptive name and press **Apply**.

Creating a descriptive input feed name:

1. Click on the **Input Feed Names** link.

2. On the subsequent **Input Feed Names** page, enter a descriptive name and press **Apply**.

Creating a descriptive outlet name:

1. Click on the **Outlet Names** link which will open the **Outlets** configuration page. See *Outlets* on page 22 for additional information on creating descriptive outlet names.

Creating a descriptive serial port name:

1. Click on the **Serial Port Names** link which will open the **Serial Port** configuration page. See *Serial Port* on page 21 for additional information on creating descriptive serial port names.

Creating a descriptive Environmental Monitor name:

1. Click on the **Environmental Monitor Names** link.
2. On the subsequent Environmental Monitor Names page, enter a descriptive name and press **Apply**.

Creating descriptive sensor names:

1. Click on the **Sensor Names** link.
2. On the **Sensor Names** page, enter a descriptive name and press **Apply**.

Network

The **Network configuration** page is used for maintenance of the network interface. From this page an administrator may configure the IP address, subnet mask and gateway address as well as view the link status, speed and duplex value.

The following network defaults allow unit configuration out-of-the-box through either Telnet/SSH or web browser:

IP address:	192.168.1.254
Subnet Mask:	255.255.255.0
Gateway:	192.168.1.1

The initial local PC network connection must be configured as noted below:

Note: *Contact your system administrator for instructions in reconfiguring the network connection. Reconfiguration of your network connection may require a restart to take effect.*

IP address:	192.168.1.x (where x is 2-253)
Subnet Mask:	255.255.255.0

Note: *The unit must be restarted after network configuration changes. See Performing a warm boot on page 57.*

Enabling or disabling DHCP support:

1. Select Enabled or Disabled from the DHCP drop-down menu and press Apply.

Setting the IP address, subnet mask, gateway or DNS address:

1. In the appropriate field, enter the IP address, subnet mask, gateway address or DNS address and press **Apply**.

Telnet/SSH

The Telnet/SSH configuration page is used to enable or disable Telnet and SSH support and configure the port number that the Telnet or SSH server watches. For more information on SSH see *Advanced Operations* on page 66.

Enabling or disabling Telnet or SSH support:

1. Select **Enabled** or **Disabled** from the appropriate Server drop-down menu and press **Apply**.

Changing the Telnet or SSH server port number:

1. In the appropriate Port field, enter the port number and press **Apply**.

Note: *The default port numbers are: port 23 for Telnet, and port 22 for SSH*.

Enabling or disabling SSH server authentication methods:
The SLP SSH server supports two authentication methods for security and validation:

Password and **Keyboard-Interactive**.

Password is an authentication method where the SSH client gathers username/password credentials and makes the authentication request to the SSH server with the credentials. The Password method is controlled by the SSH client.

Keyboard-Interactive is an authentication method where the SSH server controls an information field followed by one or more prompts requesting credential information from the SSH client. The client gathers credential information keyed-in by the user and sends it back to the server. The Keyboard-Interactive method is controlled by the SSH server.

Individual enabling and disabling of the Password and Keyboard-Interactive authentication methods are supported to allow an SSH client to be forced to use a specific method. Although both methods are available, by enabling the Keyboard-Interactive method and disabling the Password method, the SSH client is forced to used Keyboard-Interactive, which is required to display the login banner.

Note: At least one authentication method must be enabled.

1. Select the **Password** checkbox and/or the **Keyboard-Interactive** checkbox and press **Apply**.

HTTP/SSL

The HTTP/SSL configuration page is used to enable or disable HTTP and SSL support, configure the port number that the HTTP server watches and responds to, selection of the method of authentication used and SSL access level. For more information on SSL see *Advanced Operations* on page 65.

Enabling or disabling HTTP or SSL support:

1. Select Enabled or Disabled from the appropriate Server drop-down menu and press **Apply**.

Changing the HTTP server port number:

1. In the HTTP Port field, enter the port number and press **Apply**.

Note: *The default port number for HTTP is 80.*

Setting the HTTP authentication method:

The HTTP server supports two authentication methods for security and validation of the username-password – Basic and MD5 digest.

The Basic method utilizes Base64 encoding to encode and deliver the username-password over the network to the HTTP server for decoding and authentication. This basic method is supported by all web browsers and offers a minimum level of security.

Note: *The Base64 algorithm is widely-known and susceptible to packet-sniffer attack for acquisition of the encoded username-password string.*

The MD5 digest method provides stronger protection utilizing one-way encoded hash numbers, never placing the username-password on the network. Instead, the sending browser creates a challenge code based on the hash algorithm, provided username-password and unique items such as the device IP address and timestamp, which is compared against the HTTP server internal user database of valid challenge codes. The MD5 digest method offers a higher level of security than the Basic method but at present is not supported by all browsers.

Note: *MD5 is known to be fully supported by Internet Explorer 5.0+*

Select Basic or MD5 from the Authentication drop-down menu and press **Apply**.

Setting SSL access level

SSL access may be configured as optional or required. The default access level is set to optional.

Optional –Both non-secure (HTTP) and SSL encrypted connections (HTTPS) are allowed access.

Required – ONLY SSL encrypted connections (HTTPS) are allowed access.

Select **Optional** or **Required** from the Secure Access drop-down menu and press **Apply**.

Serial Port

The Serial Port configuration page is used for maintenance of the serial port.

Setting the data rate for all serial ports:

1. Select the serial port data rate from the drop-down menu and press **Apply**.

Note: *The default values are 9600 baud, 8 data bits, 1 stop bit, and no parity (9600 N 8 1).*

Setting the serial port timeout value:

1. Enter the timeout value (in minutes) in the Connection Timeout field and press **Apply**.

Creating a descriptive serial name:

1. Click on the **Edit** link in the Action column next to the port to be configured.

2. On the subsequent **Serial Port Edit** page, enter the descriptive name. Up to 24 alphanumeric and other typeable characters (ASCII 33 to 126 decimal, spaces and colon characters are not allowed) are allowed. Press **Apply**.

Note: *Port names '1' thru '64' and 'CONSOLE' are reserved system names and may not be used.*

Enabling or disabling serial port active signal checking:

1. Click on the **Edit** link in the Action column next to the port to be configured.
2. On the subsequent **Serial Port Edit** page, select On or Off from the DSR Check drop-down menu and press **Apply**.

Outlets

The **Outlets configuration** page is used for assignment and/or editing of outlet descriptive names and wakeup states.

Setting the outlet sequencing interval:

1. Enter the sequencing interval (in seconds) in the Sequencing Interval field and press **Apply**.

Setting the outlet reboot delay:

2. Enter the reboot interval (in seconds) in the Reboot Delay field and press **Apply**.

Editing the outlet descriptive name:

1. Click on the **Edit** link in the Action column next to the outlet to be configured.
2. On the subsequent **Outlet Edit** page, enter the descriptive name. Up to 24 alphanumeric and other typeable characters (ASCII 33 to 126 decimal, spaces and colon characters are not allowed) are allowed. Press **Apply**.

Changing the outlet wakeup state:

1. Click on the **Edit** link in the Action column next to the outlet to be configured.
2. On the subsequent **Outlet Edit** page, select On, Off, or Last from the Wakeup State drop-down menu and press **Apply**.

Setting the outlet Post-On delay:

3. Click on the **Edit** link in the Action column next to the outlet to be configured.
4. On the subsequent **Outlet Edit** page, enter the outlet Post-On delay (in seconds) in the Post-On Delay field and press **Apply**.

Groups

The Groups configuration page is used for creation and deletion of group and assignment of outlets to groups.

Creating a group:

1. Enter a descriptive group name in the Group Name field. Up to 24 alphanumeric and other typeable characters (ASCII 33 to 126 decimal, spaces and colon characters are not allowed) are allowed. Press **Apply**.

Removing a group:

1. Click on the **Remove** link in the Action column for the group to be removed and press **Yes** on the subsequent confirmation window.

Adding and Deleting outlets from a group:

1. Press the **Edit** link in the Action column for the associated group.
2. On the subsequent **Group Edit** page, select or deselect outlets to be included in that group. Press **Apply**.

Users

The **Users configuration** page is used for creation and removal of usernames, assignment of accessible outlets and group, assignment of privilege levels and the changing of user passwords.

Creating a new user:

1. Enter a user name in the Username field. Up to 24 alphanumeric and other typeable characters (ASCII 33 to 126 decimal, spaces and colon characters are not allowed) are allowed.
2. Enter a password for the new user in the Password and Verify Password fields. For security, password characters are not displayed. Press **Apply**.

Removing a user:

1. Click on the **Remove** link in the Action column for the user to be removed and press **Yes** on the subsequent confirmation window.

Changing a user password:

1. Click on the **Edit** link in the Action column for the associated user.
2. On the subsequent **User Edit** page, enter the new password in the Password and Verify Password fields. For security, password characters are not displayed. Press **Apply**.

Changing a user's access privilege level:

There are six defined access privilege levels; Admin, Power User, User, Reboot-Only, On-Only and View-Only:

- Admin: Full-access for all configuration, control (On, Off, Reboot) , status and serial/Pass-Thru ports.
- Power User: Full-access for all control (On, Off, Reboot), status and serial/Pass-Thru ports.
- User: Partial-access for control (On, Off, Reboot), status of assigned outlets, groups and serial/Pass-Thru ports.
- Reboot-Only: Partial access for control (Reboot), status and Pass-Thru of

assigned outlets, groups and serial/Pass-Thru ports.

- On-Only: Partial-access for control (On) , status and Pass-Thru of assigned outlets, groups and serial/Pass-Thru ports.
- View-Only: Partial-access for status and Pass-Thru of assigned outlets, groups and serial/Pass-Thru ports.

The administrator may also grant administrative privileges to other user accounts, allowing the SLP to have more than one administrative-level user.

Note: *You cannot remove administrative privileges from the Admin user unless another user has already been given administrative access level privileges created.*

1. Click on the **Edit** link in the Action column for the associated user.
2. On the subsequent User Edit page, select **Admin**, **Power-User**, **User**, **Reboot-Only, On-only** or **View-Only** from the Access Level drop-down menu and press **Apply**.

Granting or removing Environmental Monitoring viewing privileges:

1. Click on the **Edit** link in the Action column for the associated user.
2. On the subsequent **User Edit** page, select Yes or No from the Environmental Monitoring drop-down menu and press **Apply**.

Adding and Deleting outlet access:

1. Click on the **Outlets** link in the Access column for the associated user.
2. On the subsequent **User Outlets** page, select or deselect outlets to be accessed by the user and press **Apply**.

Adding and Deleting group access:

1. Click on the **Groups** link in the Access column for the associated user.
2. On the subsequent **User Groups** page, select or deselect group to be accessed by the user and press **Apply**.

Adding and deleting serial port access:

1. Click on the **Ports** link in the Access column for the associated user.
2. On the subsequent **User Ports** page, select or deselect ports to be accessed by the user and press **Apply**.

FTP

The FTP configuration page is used for setup and maintenance of all settings required to perform an FTP firmware upload. See Uploading Firmware on page [100] for more information on uploading firmware.

Setting the FTP Host IP Address:

1. Enter the IP address in the Host IP Address field and press **Apply**.

Setting the FTP username:

1. Enter the FTP server username in the Username field, and press **Apply**.

Setting the FTP password:

1. Enter the FTP server password in the Password field, and press **Apply**.

Setting the file path:

1. Enter the path of the file to be uploaded in the Directory field, and press **Apply**.

Setting the filename for upload:

1. Enter the filename of the file to be uploaded in the Filename field, and press **Apply**.

Testing the FTP upload configuration:

This test validates that the unit is able to contact and log onto the specified FTP server, download the firmware file and verify that the firmware file is valid for this unit.

1. Press **Test**.

Enabling or disabling automatic updates:

The SLP features the ability to schedule automation firmware updates. When enabled the SLP will regularly check the FTP servers for a new firmware image and upload it.

1. Select **Enabled** or **Disabled** from the drop-down menu and press **Apply**.

Setting the automatic update scheduled day:

1. Select the desired day for the automatic update from the drop-down menu and press **Apply**.

Setting the automatic update scheduled hour:

1. Select the desired hour for the automatic update from the drop-down menu and press **Apply**.

Enabling or disabling the FTP server:

The SLP features the ability to upload and download system configuration files to ease implementation across multiple SLP devices. See Advanced Operations for more information on configuration upload and download.

1. Select **Enabled** or **Disabled** from the drop-down menu and press **Apply**.

Note: *The FTP server must be enabled for configuration upload or download.*

SNTP/Syslog

3. The SNTP/Syslog configuration page is used for setup and maintenance of SNTP and Syslog support. For additional information and configuration requirements for Syslog support, see

Logging *on page* 93.

Setting the SNTP server address:

1. Enter the IP address or hostname in the Primary and/or Secondary Host field and press **Apply**.

Setting the Local GMT offset:

1. Select the local offset from GMT value from the drop-down menu and press **Apply**.

Setting the Syslog server address:

1. Enter the IP address or hostname in the Primary and/or Secondary Host field and press **Apply**.

Changing the Syslog server port number:

1. In the Syslog Port field, enter the port number and press **Apply**.

SNMP

The **SNMP configuration** page is used for setup and maintenance of all settings required to enable SNMP support as well as access to the trap configuration pages. For additional information on SNMP support and detailed descriptions of available traps, see *SNMP* on page 68.

Note: *Traps are generated according to a hierarchical architecture; i.e. if a Tower (Unit) Status enters a trap condition, only the Tower Status trap is generated. Infeed and Outlet Status traps are suppressed until the Tower Status returns to Normal.*

Enabling or disabling SNMP support:

1. Select Enabled or Disabled from the drop-down menu and press **Apply**.

Setting the community strings:

1. Enter the community string in the appropriate field and press **Apply**.

   Community strings may be 1 to 24 characters

Setting the trap timer:

1. Enter a trap timer value in the Error Trap Repeat Time field and press **Apply**.

   The Error Trap Repeat Time value may be 1 to 65535 (in seconds).

Setting trap destinations:

1. Enter an IP address or hostname in the appropriate Trap Destination field and press **Apply**.

Setting *IP restrictions*:

1. Select **No Restrictions** or **Trap Destinations Only** from the IP Restrictions drop-down menu and press **Apply**.

Note: *When Trap Destinations Only is selected, SNMP Manager GET and SET requests are only allowed from the IP addresses of the defined traps destinations.*

Setting the SNMP SysName, SysLocation or SysContact objects:

1. In the appropriate field, enter the SysName, SysLocation or SysContact objects and press **Apply**.

Enabling or disabling tower (unit) traps:

1. Click on the **Tower Traps** link.
2. On the subsequent page, select or deselect the desired traps and press **Apply**.

Configuring input feed traps:

1. Click on the **Input Feed Traps** link.
2. On the subsequent **Input Feed Traps** page, select or deselect the desired traps and press **Apply**.
3. For Load traps, enter a maximum load value for the infeed in the High Load Threshold field and press **Apply**.

   The High Load Threshold value may be 0 to 255 (in amperes).

Configuring outlet traps:

1. Click on the **Outlet Traps** link.
2. On the subsequent **Outlet Traps** page, select or deselect the desired traps and press **Apply**.

Enabling or disabling Environmental Monitor traps:

1. Click on the **Environmental Monitor Traps** link.
2. On the subsequent page, select or deselect the desired traps and press **Apply**.

Configuring the Temperature-Humidity sensor traps:

1. Click on the **Sensor Traps** link.
2. On the subsequent page, select or deselect the desired traps and press **Apply**.
3. For Temp traps, enter a minimum and maximum threshold value for the sensor in the appropriate field and press **Apply**.
   The threshold value may be 0 to 127 degrees Celsius OR 32 to 254 degrees Fahrenheit.
4. For Humid traps, enter a minimum and maximum threshold value for the sensor in the appropriate field and press **Apply**.
   The threshold value may be 0 to 100 (in percent relative humidity).

LDAP

The **LDAP** configuration page is used for setup and maintenance of all settings required to enable LDAP support. For additional information and configuration requirements, see LDAP on page 76.

Enabling or disabling LDAP support:

1. Select **Enabled** or **Disabled** from the LDAP drop-down menu and press **Apply**.

Changing the LDAP server port:

1. Enter the port number in the LDAP Port field and press **Apply**.

Setting the LDAP server address:

1. Enter the IP address or hostname in the Primary and/or Secondary Host field and press **Apply**.

Note: *If LDAP over TLS/SSL is enabled, MD5 binding is disabled.*

Enabling or disabling LDAP over TLS/SSL:

1. Select **Yes** or **No** from the Use TLS/SSL drop-down menu and press **Apply**.

Setting the LDAP bind password type:

1. Select **Simple** or **MD5** from the Bind Type drop-down menu and press **Apply**.

Note: *If MD5 binding is enabled, LDAP over TLS/SSL is disabled.*

For more information on LDAP bind password types, see Setting the LDAP bind password type on page 79.

Setting the search bind Distinguished Name (DN):

1. Enter the fully-qualified distinguished name (FQDN) in the Search Bind field and press **Apply**.

Setting the search bind password for Distinguished Name (DN):

1. Enter the Search Bind password in the Search Bind Password field and press **Apply**.

Setting the user search base Distinguished Name (DN):

1. Enter the User Search Base DN in the User Search Base DN field and press **Apply**.

Setting the user search filter:

1. Enter the User Search Filter in the User Search Filter field and press **Apply**.

Setting the group membership attribute:

1. Enter the group membership attribute in the Group Membership Attribute Field and press **Apply**.

Setting the group membership value type:

1. Select the appropriate value from the drop-down menu and press **Apply**.

Configuring the authentication order:

1. Select **Remote -> Local** or **Remote Only** from the drop-down menu and press **Apply**.

Note: *Lantronix recommends NOT setting the authentication order to Remote Only until the LDAP has been fully configured and tested.*

Configuring LDAP groups:

1. Click on the **LDAP Groups** at the bottom of the page.

Creating an LDAP group:

1. Enter a descriptive group name in the **LDAP Group Name field.** Up to 24 alphanumeric and other typeable characters (ASCII 33 to 126 decimal) are allowed; spaces are not allowed. Press **Apply**.

Removing an LDAP group:

1. Click on the **Remove** link in the Action column for the group to be removed and press **OK** on the subsequent confirmation window.

Changing and LDAP group's access privilege level:

1. Click on the **Edit** link in the Action column for the associated LDAP Group.
2. On the subsequent LDAP Group-edit page, select **Admin, User, On-Only** or **View-Only** from the Access Level drop-down menu and press **Apply**.

For more information on access privilege levels, see Users on page 23.

Granting or removing Environmental Monitoring viewing privileges:

1. Click on the **Edit** link in the Action column for the associated LDAP Group.
2. On the subsequent LDAP Group-edit page, select **Yes** or **No** from the Environmental Monitoring drop-down menu and press **Apply**.

Adding and Deleting outlet access:

1. Click on the **Outlets** link in the Action column for the associated LDAP Group.
2. On the subsequent LDAP Group-Outlets page, select or deselect outlets to be accessed by the LDAP Group and press **Apply**.

Adding and Deleting outlet group access:

1. Click on the **Groups** link in the Action column for the associated LDAP Group.
2. On the subsequent LDAP Group-Groups page, select or deselect outlet groups to be accessed by the LDAP Group and press **Apply**.

Adding and Deleting serial port access:

1. Click on the **Ports** link in the Action column for the associated LDAP Group.
2. On the subsequent LDAP Group-Ports page, select or deselect ports to be accessed by the LDAP Group and press **Apply**.

TACACS+

The TACACS+ configuration page is used for setup and maintenance of all settings required to enable TACACS+ support. For additional information and configuration requirements, see TACACS+ on page 29.

Enabling or disabling TACACS+ support:

1. Select **Enabled** or **Disabled** from the TACACS+ drop-down menu and press **Apply**.

Setting the TACACS+ server address:

1. Enter the IP address or hostname in the Primary and/or Secondary Host field and press **Apply**.

Changing the TACACS+ server port:

1. Enter the port number in the Port field and press **Apply**.

Configuring the authentication order:

1. Select **Remote -> Local** or **Remote Only** from the drop-down menu and press **Apply**.

For more information on remote authentication order, see Setting the authentication order:on page 88.

Note: *Lantronix recommends NOT setting the authentication order to Remote Only until the TACACS+ has been fully configured and tested.*

Setting the TACACS+ encryption key:

1. Enter a key and verify the new key, the Encryption Key and Verify Encryption Key fields. Press **Apply**.

   For security, key characters are not displayed.

Configuring the TACACS+ privilege levels:

1. Click on the **TACACS+ Privilege Levels** link at the bottom of the page.

Changing a TACACS+ Privilege Level's access privilege level:

1. Click on the **Edit** link in the Action column for the associated TACACS+ Privilege Level.
2. On the subsequent TACACS+ Privilege Level-Edit page, select **Admin, User, On-Only** or **View-Only** from the Access Level drop-down menu and press **Apply**.

For more information on access levels, see Users on page 23.

Granting or removing Environmental Monitoring viewing privileges:

1. Click on the **Edit** link in the Action column for the associated TACACS+ Privilege Level.
2. On the subsequent TACACS+ Privilege Level-Edit page, select **Yes** or **NO** from the **Environmental Monitoring** drop-down menu and press **Apply**.

   Adding and Deleting outlet access:

3. Click on the **Outlets** link in the Action column for the associated TACACS+ Privilege Level.

4. On the subsequent LDAP Group-Outlets page, select or deselect outlets to be accessed by the TACACS+ Privilege Level and press **Apply**.

Adding and Deleting outlet group access:

3. Click on the **Outlets** link in the Action column for the associated TACACS+ Privilege Level.
4. On the subsequent LDAP Group-Groups page, select or deselect outlet groups to be accessed by the TACACS+ Privilege Level and press **Apply**.

Adding and Deleting serial port access:

3. Click on the **Ports** link in the Action column for the associated TACACS+ Privilege Level.
4. On the subsequent LDAP Group-Ports page, select or deselect ports to be accessed by the TACACS+ Privilege Level and press **Apply**.

Email

The Email configuration page is used for setup and maintenance of Email log support. For additional information and configuration requirements for Email support, see

Logging on page 93.

Enabling or disabling Email support:

1. Select **Enabled** or **Disabled** from the Email Notifications drop-down menu and press **Apply**.

Setting the SMTP server address:

1. Enter the IP address or hostname in the SMTP Host field and press **Apply**.

Changing the SMTP server port:

1. Enter the port number in the SMTP Port field and press **Apply**.

Setting the 'From' email address:

1. Enter the 'from' email address in the 'From' Address field and press **Apply**.

Setting the 'To' email address:

1. Enter the 'to' email address in the 'Send To' Address field and press **Apply**.

Enabling or Disabling event type notifications:

1. Select **Enabled** or **Disabled** from the Include…Messages drop-down menus and press **Apply**.

Tools

The Tools section contains access to rebooting the unit, uploading new firmware as well as resetting the unit to factory defaults. This section is available to administrative level users only.

Ping

The Ping feature may be used to test the SLP's ability to contact another Ethernet enabled device's IP address. For LDAP support, it may also be used to test the configuration of the Domain Name server IP address by testing for proper name resolution.

Change Password

The Change Password feature allows users to change their own password.

Note: *An administrator can always assign a new password.*

Changing a password:

1. Enter the current password, enter a new password and verify the new password. Press **Apply**.

View Log

The View Log feature enables viewing of the internal system log. This feature logs all authentication attempts, power actions, configuration changes and other system events. The system memory stores more than 4000 entries in a continuously aging log. For permanent off-system log storage, the Syslog protocol is supported. For additional information and configuration requirements for the system log and Syslog support, see

Logging on page 93.

Note: *The system log is viewable only by users with administrative privileges.*

Reviewing the system log:

Click on the **Previous 200 entries** or **Next 100 entries** link to navigate through the log.

Restart

Performing a warm boot:

1. Select the **Restart** from the Action drop-down menu and press **Apply**.

Note: *System user/outlet/group configuration or outlet states are NOT changed or reset with this command.*

Resetting to factory defaults:

See *Resetting to Factory Defaults* for more information on resetting a unit to factory defaults from the HTML interface.

Uploading new firmware:

See *Uploading Firmware* for more information on uploading new firmware from the HTML interface.

Generating a new SSL X.509 certificate:

Select the **Restart and generate a new X.509 certificate** from the Action drop-down menu and press **Apply**.

Computing new SSH security keys:

1. Select the **Restart and compute new SSH keys** from the Action drop-down menu and press **Apply**.

Command Line Interface

Logging In

Logging in through Telnet/SSH requires directing the Telnet/SSH client to the configured IP address of the unit.

Logging in through the Console (RS-232) port requires the use of a terminal or terminal emulation software configured to support ANSI or VT100 and a supported data rate (300, 1200, 2400, 4800, 9600, 19200, 38400, 57600, or 115200 BPS) - 8 data bits-no parity-one stop bit and Device Ready output signal (DTR or DSR).

To log in by RS-232 or Telnet/SSH:

1. **Press Enter**. The following appears, where x.xx is the firmware version:

```
SecureLinx Power Manager Version x.xx
Username:
```

Note: *Logging in by Telnet will automatically open a session. It is not necessary to press* ***Enter****.*

2. At the `Username` and `Password` prompts, enter a valid username and password. And press **Enter**.

   You are given three attempts to enter a valid username and password combination. If all three fail, the session ends.

   When you enter a valid username and password, the command prompt `SLP:` appears. If a location identifier was defined, it will be displayed before the prompt. See *Creating a pre-login banner*

The Set Banner command specifies text that appears prior to the login authentication. This feature allows administrators to configure a message up to 2070 characters for display of legal, disclaimer or other text as required by application. If left blank, the user will be taken directly to the login prompt.

Note: *For SSH sessions, the 'keyboard interactive' authentication method must be used for the banner to display.*

To create a pre-login banner:

1. At the command prompt, type **`set banner`** and press **Enter.** Type the desired pre-login banner text and when finished type Ctrl-z.

   Creating a location description on page 52 for more information.

You may enter commands in any combination of uppercase and lowercase. You must enter all command characters correctly; there are no command abbreviations. There are two types of commands: operations and administration. A user must have administrative privileges to use the administration commands. The following tables list and briefly describe each command.

Table 3-2. Operations Command Summary

Command	Description
On	Turns one or more outlets on
Off	Turns one or more outlets off
Reboot	Reboots one or more outlets
Status	Displays the on/off status of one or more outlets
ILoad	Displays the total cumulative input load
IStat	Displays the status of the infeed
Connect	Connect to the serial port
Login	Ends the current session and brings up the Username prompt
Logout	Ends a session
Password	Changes the password for the current user
Quit	Ends a session
List Outlets	Lists all accessible outlets for the current user
List Ports	Lists all accessible serial/Pass-Thru ports for the current user
List Group	Lists all assigned outlets for a group name
List Groups	Lists all accessible groups for the current user

Table 3-3. Administrative Command Summary

Command	Description
Add Grouptouser	Grants a user access to one or more groups
Add Outlettogroup	Adds an outlet to a group name
Add Outlettouser	Grants a user access to one or all outlets
Add Portuser	Grants a user access to one or all serial/Pass-Thru ports
Create Group	Adds a group name
Create User	Adds a user account
Delete Groupfromuser	Removes access to one or more groups for a user
Delete Outletfromgroup	Deletes an outlet from a group name
Delete Outletfromuser	Removes access to one or all outlets for a user
Delete Portfromuser	Removes access to one or all serial/Pass-Thru ports
List User	Displays all accessible outlets/groups for a user
List Users	Displays privilege levels for all users
Remove Group	Deletes a group name
Remove User	Deletes a user account
Restart	Performs a warm boot
Set Banner	Set the pre-login banner text
Set DHCP	Enables or disables DHCP support
Set DNS	Sets the IP address of the Domain Name server
Set FTP Autoupdate	Enables or disables automatic FTP update support
Set FTP Autoupdate Day	Sets the automatic FTP update day

Command	Description
Set FTP Autoupdate Hour	Set the automatic FTP udate hour
Set FTP Directory	Specifies the directory for the file to be uploaded
Set FTP Filename	Specifies the file to be uploaded via FTP
Set FTP Filepath	Specifies the file path for the file to be uploaded
Set FTP Host	Sets the FTP Host IP address
Set FTP Password	Sets the password for the FTP Host
Set FTP Username	Sets the username for the FTP Host
Set FTP Server	Enables or disables the FTP server
Set Gateway	Sets the Gateway
Set HTTP	Enables or disables HTTP access
Set HTTP Port	Specifies the target port for HTTP access
Set HTTP Security	Specifies the HTTP server authentication method
Set Infeed Name	Specifies a descriptive field for the infeed
Set Ipaddress	Sets the IP address
Set Location	Specifies a descriptive field for the web browser control screen and login banner
Set Option Button	Enables or disables the external configuration reset button
Set Option Display	Sets the LED orientation for the external Current displays
Set Option More	Enables or disables the ‘more’ prompt
Set Option StrongPasswords	Enables or disables strong password requirements
Set Option Tempscale	Sets the Environmental Monitor temperature scale
Set Outlet Name	Specifies a descriptive field for a device attached to an outlet
Set Outlet PostOnDelay	Sets the Post-On delay for an outlet
Set Outlet RebootDelay	Sets the reboot delay for all outlets
Set Outlet SeqInterval	Sets the sequencing interval for all outlets
Set Outlet Wakeup	Sets the wakeup state for an outlet
Set Port Name	Specifies a descriptive field for the serial port
Set Port Dsrchk	Sets the DSR active signal checking for a serial/Pass-Thru port
Set Port Speed	Set the connection speed for the serial port
Set Port Timeout	Sets the activity timer for Pass-Thru sessions
Set SNTP	Sets the IP address or hostname of the SNTP servers
Set SNTP GMTOffset	Sets the local GMT offset applied to the SNTP servers
Set Subnet	Sets the Subnet Mask of the SLP
Set Telnet	Enables or disables Telnet access
Set Telnet Port	Sets the Telnet server port number
Set Tower Name	Specifies a descriptive field for the SLP
Set User Access	Sets the access level for a user
Set User Envmon	Grants or removes privileges to view input and environmental monitoring status
Set User Password	Changes the password for a user
Show FTP	Displays FTP configuration information
Show Infeeds	Displays infeed configuration information

Command	Description
Show Network	Display network configuration information
Show Outlets	Displays configuration information for all outlets
Show Ports	Displays the serial port configuration information
Show System	Displays system configuration information
Show Towers	Displays unit configuration information
Version	Displays the firmware version

To display the names of commands that you may execute:

1. At the command prompt, press **Enter**. A list of valid commands for the current user appears.

Operations Commands

Operations commands manage outlet states, provide information about the unit's environment and control session operations.

Note: *Users must be granted access to affect any change in outlet state.*

Turning outlets on

The On command turns on one or more outlets. When the command completes, a display indicating all outlets affected and their current states will be displayed.

To turn outlets on:

1. At the command prompt, type `on`, followed by one or more outlet names separated by spaces or commas, and press **Enter**, or
2. Type `on`, followed by a group name, and press **Enter**, or
3. Type `on all` and press **Enter**.

Examples

The following command turns the second outlet on, using the outlet's absolute name:

```
SLP: on .a2<Enter>
```

The following command turns on all the outlets in the group named ServerGroup_1:

```
SLP: on ServerGroup_1<Enter>
```

Turning outlets off

The Off command turns off one or more outlets. When the command completes, a display indicating all outlets affected and their current states will be displayed.

To turn outlets off:

1. At the command prompt, type `off`, followed by one or more outlet names separated by spaces or commas, and press **Enter**, or
2. Type `off`, followed by a group name, and press **Enter**, or
3. Type `off all` and press **Enter**.

Examples

The following command turns off the outlet named FileServer_1:

```
SLP: off FileServer_1<Enter>
```

The following command turns off all outlets:

```
SLP: off all<Enter>
```

Rebooting outlets

The Reboot command reboots one or more outlets. This operation turns the outlet(s) off, delays for a period of 15 seconds and then turns the outlet(s) on. When the command completes, a display indicating all outlets affected and their current states will be displayed.

Note: *It is necessary to reissue the Status command to verify that the outlets have rebooted after 15 seconds.* *See Displaying outlet information on page 50 for more information.*

To reboot one or more outlets:

1. At the command prompt, type `reboot`, followed by one or more outlet names separated by spaces or commas, and press **Enter**, or
2. Type `reboot`, followed by a group name, and press **Enter**, or
3. Type `reboot all` and press **Enter**.

Example

The following command reboots all the outlets in the group named ServerGroup_1:

```
SLP: reboot ServerGroup_1<Enter>
```

Displaying outlet status

The Status command displays the on/off status of one or more outlets. The command displays the status of only those outlets for which the current username has power control access.

This display includes the outlet absolute and descriptive names, the Outlet State reported to the unit by the outlet and the current Control State being applied by the unit. If you do not specify any parameter with this command, the status of all accessible outlets is displayed.

Note: *If the user has access to more than 16 total outlets, the Status command will display the first 16 outlets with a prompt to view the remaining outlets.*

For more information on outlet and control state values, see *Outlet Control* on page 15.

To display on/off status of one or more outlets:

1. At the command prompt, type `status`, followed by an outlet name, and press **Enter**, or
2. Type `status`, followed by a group name, and press **Enter**, or
3. Type `status` and press **Enter**.

Examples

The following command displays the on/off status of the outlet named FileServer_1:

```
SLP: status FileServer_1<Enter>
   Outlet   Outlet                    Outlet   Control
   ID       Name                      State    State
   .A3      FileServer_1              On       On
```

The following command displays the on/off status of all accessible outlets:

```
SLP: status<Enter>
   Outlet   Outlet                    Outlet
Control
   ID       Name                      State    State
   .A1      DataServer_1              On       On
   .A2      WebServer_1               On       On
   .A3      FileServer_1              On       On
   .A4                                On       On
   .A5                                On       On
   .A6                                On       On
   .A7                                On       On
   .A8                                On       On
   .A9                                On       On
   .A10                               On       On
   .A11                               On       On
   .A12                               On       On
   .A13                               On       On
   .A14                               On       On
   .A15                               On       On
   .A16                               On       On
   More (Y/es N/o):
```

The following command displays the on/off status for outlets in the group ServerGroup_1:

```
SLP: status ServerGroup_1<Enter>
   Group: ServerGroup_1
      Outlet   Outlet                    Outlet   Control
      ID       Name                      State    State
      .A1      DataServer_1              On       On
      .A2      WebServer_1               On       On
      .A3      FileServer_1              On       On
```

Displaying accessible outlets

The List Outlets command displays accessible outlets for the current user. The display includes the absolute and descriptive name of all outlets assigned to the current user.

To display accessible outlets:

1. At the command prompt, type `list outlets` and press **Enter**.

Example

The following command displays all accessible outlets for the current user:

```
SLP:list outlets<Enter>
   Outlet   Outlet
   ID       Name
   .A1      DataServer_1
   .A2      WebServer_1
```

Displaying accessible groups

The List Groups command displays accessible groups for the current user.

To display accessible groups:

1. At the command prompt, type `list groups` and press **Enter**.

Example

The following command displays all accessible groups for the current user:

```
SLP: list groups<Enter>
   Groups:
      ServerGroup_1
      RouterGroup_1
```

Displaying outlets assigned to a group

The List Group command displays outlets assigned to the specified group name.

To display outlets assigned to a group:

1. At the command prompt, type `list group`, followed by the group name and press **Enter**.

Example

The following command displays the outlets assigned to the group ServerGroup_1:

```
SLP: list group ServerGroup_1<Enter>
   Group: ServerGroup_1
      Outlet   Outlet
```

```
      ID        Name
      .A1       DataServer_1
      .A2       WebServer_1
      .A3       FileServer_1
```

Displaying accessible serial ports

The list ports command displays accessible serial ports for the current user.

To display accessible serial ports:

1. At the SLP prompt, type **list ports** and press **Enter**.

   Example

   The following command displays all accessible serial ports for the current user:

```
SLP: list ports <Enter>
   Port         Port
   ID           Name
   Console      Console
```

Displaying infeed status

The Istat or Iload command displays the status of one or more infeed.

This display includes the infeed absolute and descriptive names and the Input Status and current Load reported to the unit by the infeed.

To display status of one or more infeeds:

1. Type `istat` and press **Enter**, or
2. Type `iload` and press **Enter**.

Examples

The following command displays the infeed status:

```
SLP: istat
   Input    Input                    Input      Input
   Feed ID  Feed Name                Status     Load
   .AA      HQ_1_Infeed_A            On         10.5 Amps
```

Connecting to a serial device

The Connect command allows serial connection to devices attached to one of the two standard serial ports (Console, Modem).

To connect to a serial device:

1. At the SLP prompt, type **connect,** followed by the serial port name and press **Enter**.

To disconnect from a serial device:

1. Type **!*break** and press **Enter**.

Displaying the status of the Environmental Monitor:

The Envmon command displays the status of the integrated Environmental Monitor.

By default, only administrative user accounts are allowed access to the Envmon command. An administrator may user the Set User Envmon command to enable and disable access for other user accounts.

To display the status of the Environmental Monitor:

At the SLP: prompt, type **envmon** and press **Enter**.

Example

The following command displays the status of the Environmental Monitor.

```
SLP: envmon<Enter>
Environmental Monitor .A
   Name: Florida_HQ_1                    Status: Normal
   Temperature/Humidity Sensors
      ID    Name                         Temperature    Humidity
      .A1   Temp_Humid_Sensor_A1         Not Found      Not Found
      .A2   T/H2_Florida_HQ_1            23.5 Deg. C    22 % RH
```

Changing a password

The Password command changes the current user's password. For security, when you type a password the characters are not displayed on the screen. See Usernames and Passwords for more information.

To change a password:

1. At the SLP prompt, type **password** and press **Enter**.
2. At the Enter Current Password prompt type the current password and press **Enter**.
3. At the Enter New Password prompt type the new password and press **Enter**. Passwords may contain 1-16 characters.
4. At the Verify Password prompt retype the new password and press **Enter**.

Starting a new session

The Login command activates the `Username` prompt. The current session ends, allowing a user to log in and start a new session under a different username.

To start a new session:

2. At the command prompt, type `login` and press **Enter**. The `Username` prompt appears.

Ending a session

The Quit or Logout commands end a session. A session ends automatically when no activity is detected for five minutes, or upon loss of connection.

To end a session:

1. At the command prompt, type `quit` and press **Enter**, or
2. Type `logout` and press **Enter**.

Administration Commands

Administration commands may only be issued by a user with administrative privileges, such as the predefined administrative account or another user who has been granted administrative privileges with the Set User Admnpriv command.

User Administration

Creating a user account

The Create User command creates a user account with the specified username and password.

To create a user account:

1. At the command prompt, type `create user`, optionally followed by a 1-16 character username (Spaces are not allowed, and usernames are not case sensitive). Press **Enter**.
2. At the `Password` prompt, type a password of up to 16 alphanumeric and other typeable characters (ASCII 32 to 126 decimal). Passwords are case sensitive. Press **Enter**.
3. At the `Verify Password` prompt, retype the password. Press **Enter**.

Example

The following command creates the user account JaneDoe:

```
SLP: create user JaneDoe<Enter>
Password: <Enter>
Verify New Password: <Enter>
```

For security, password characters are not displayed.

Removing a user account

The Remove User command removes a user account.

Note: *You may remove the predefined user account Admn only if another user account has been granted administrative privileges using the Set User Access command.*

To remove a user account:

1. At the command prompt, type `remove user`, optionally followed by a username. Press **Enter**.

Changing a password

The Set User Password command changes a user's password. For security, when you type a password, the characters are not displayed on the screen.

To change a password:

1. At the command prompt, type `set user password`, followed by a username and press **Enter**.
2. At the `Password` prompt, type the new password and press **Enter**. Passwords may contain up to 16 characters, and spaces are not allowed.

3. At the `Verify Password` prompt, retype the new password and press **Enter**.

Examples

The following command changes the password for the user JohnDoe:

```
SLP: set user password johndoe<Enter>
   Password: <Enter>
   Verify Password: <Enter>
```

Setting user access level privileges

The Set User Access command sets the access level privileges for a user. There are four defined access privilege levels; Admin, User, On-Only and View-Only.

The administrator may also grant administrative privileges to other user accounts allowing the unit to have more than one administrative-level user.

Note: *You cannot remove administrative privileges from the Admin user unless another user has already been given administrative access privileges.*

To set the access level privilege for a user:

1. At the command prompt, type `set user access`, followed by `admn`, `user`, `ononly` or `viewonly`, optionally followed by a username and press **Enter**.

Examples

The following command sets the user access level for JohnDoe to Admin:

```
SLP: set user access admin johndoe<Enter>
```

The following command sets the user access level for JaneDoe to User:

```
SLP: set user access user janedoe<Enter>
```

Granting and removing input load viewing privileges

The Set User Envmon command grants or removes input load viewing privileges to/from a general or view-only user.

To grant or remove input load viewing privileges for a user:

1. At the command prompt, type `set user envmon` followed by on or off, optionally followed by a username and press **Enter**.

Example

The following command grants input load privileges to the user JohnDoe:

```
SLP: set user envmon on johndoe<Enter>
```

Displaying the access privilege levels

The List Users command displays all defined users with their access privilege level.

To display user access privilege levels:

1. At the command prompt, type `list users` and press **Enter**.

Example

The following command displays all users with their access privilege level:

```
SLP: list users<Enter>
   User              Privilege     Environmental
   Name              Level         Monitoring
   JOHNDOE           Admin         Allowed
   JILLDOE           Power-User    Allowed
   JANEDOE           User          Allowed
   JAKEDOE           Reboot-Only   Not Allowed
   JOSEYDOE          On-Only       Not Allowed
   JOEDOE            View-Only     Not Allowed
```

Adding outlet access to a user

The Add OutletToUser command grants a user access to one or all outlets. To grant access for more than one outlet, but not all outlets, you must use multiple Add OutletToUser commands.

To grant outlet access to a user:

1. At the command prompt, type `add outlettouser`, optionally followed by an outlet name and a username. Press **Enter**, or
2. Type `add outlettouser all`, followed by a username and press **Enter**.

Examples

The following commands grant the user JaneDoe access to outlets A1 and Webserver_1:

```
SLP: add outlettouser .a1 janedoe<Enter>
SLP:  add outlettouser WebServer_1 janedoe<Enter>
```

Deleting outlet access for a user

The Delete OutletFromUser command removes a user's access to one or all outlets. You cannot remove access to any outlet for an administrative level user.

To delete outlet access for a user:

1. At the command prompt, type `delete outletfromuser`, optionally followed by an outlet name and a username. Press **Enter**, or
2. Type `delete outletfromuser all`, followed by a username and press **Enter**.

Adding group access to a user

The Add GroupToUser command grants a user access to a group. To grant access for more than one group, you must use multiple Add GroupToUser commands.

To grant group access to a user:

1. At the command prompt, type `add grouptouser`, optionally followed by a group name and a username. Press **Enter**.

Examples

The following commands grant access to the Groups ServerGroup_1 and ServerGroup_2 for user JaneDoe:

```
SLP:  add GroupToUser ServerGroup_1 janedoe<Enter>
SLP:  add GroupToUser ServerGroup_2 janedoe<Enter>
```

Deleting group access for a user

The Delete GroupFromUser command removes a user's access to a group. You cannot remove access to any group for an administrative level user.

To delete group access for a user:

1. At the command prompt, type `delete GroupFromUser`, optionally followed by a group name and a username. Press **Enter**.

Adding serial port access to a user

The Add PortToUser command grants a user access to the serial port.

To grant serial port access to a user:

1. At the SLP prompt, type `add porttouser console` and username. Press **Enter**.

Deleting serial port access for a user

The Delete PortFromUser command removes a user's access to the serial port. You cannot remove access to the serial port for an administrative level user.

To delete serial port access for a user:

2. At the SLP prompt, type `delete portfromuser console` and username. Press **Enter**.

Displaying user outlet and group access

The List User command displays all accessible outlets and groups for a user.

To display user outlet and group access:

3. At the command prompt, type `list user`, optionally followed by a username. Press **Enter**.

Example

The following command displays information about the user JaneDoe:

```
SLP:  list user janedoe<Enter>
   Username: JANEDOE
      Outlet   Outlet
      ID       Name
      .A1      DataServer_1
      .A2      WebServer_1
      Groups:
         ServerGroup_1
         ServerGroup_2
  More (Y/es N/o): Y
     Ports:
        Port      Port
        ID        Name
        Console   Console
```

JaneDoe may access the following outlets and groups: outlet A1 which has a descriptive name of DataServer_1, outlet A2 which has a descriptive name of WebServer_1, group ServerGroup_1, group ServerGroup_2, and Console serial port.

Outlet Administration

Setting the sequencing interval

The Set Outlet SeqInterval command sets the power on sequencing interval for all outlets.

To set the sequencing interval:

1. At the SLP prompt, type `set outlet interval for all`, followed by a value from 0 to 15 (in seconds) and press **Enter**.

Setting the reboot delay

The Set Outlet RebootDelay command sets the reboot delay for all outlets.

To set the sequencing interval:

2. At the SLP prompt, type `set outlet rebootdelay all`, followed by a value from 5 to 60 (in seconds) and press **Enter**.

Creating a descriptive outlet name

The Set Outlet Name command assigns a descriptive name to an outlet. You may use this name in commands that require an outlet name as an alternative to using the outlet's absolute name.

To create an outlet name:

1. At the SLP prompt, type `set outlet name`, followed by the absolute outlet name, then a descriptive name of up to 24 alphanumeric and other typeable characters-(ASCII 33 to 126 decimal) are allowed; spaces are not allowed; outlet names are not case sensitive. Press **Enter**.

Example

The following command adds the descriptive name Data Server_1 to outlet .a1:

```
SLP: set outlet name .a1 DataServer_1<Enter>
```

Setting the outlet wakeup state

The Set Outlet Wakeup command sets the default wakeup state for that outlet. In the event of a system-wide power loss, this state will be applied to the outlet when power is restored.

The wakeup state may be set to On, Off or Last. Upon restoration of system power; If set to ON, the SLP will apply power to that outlet. If set to Off, the SLP will not apply power to that outlet. If set to Last, the SLP will apply the last known power state.

To set the wakeup state:

1. At the SLP prompt, type `set outlet wakeup`, followed by **on**, **off** or **last** and the outlet name. Press **Enter**.

Example

The following command sets the wakeup state for outlet .a1 to off:

```
SLP: set outlet wakeup off .a1<Enter>
```

Setting the outlet Post-On delay

The Set Outlet PostOnDelay command sets the Post-On delay for an outlet. This feature allows and administrator to manage boot dependencies during power-on sequencing or group commands by delaying the sequencing of subsequent outlets after an outlet has been powered on.

Note: *This delay is applied in addition to the general sequencing interval.*

To set the Post-On delay:

2. At the SLP prompt, type `set outlet postondelay`, followed by a value from 0 to 900 (in seconds) and press **Enter**.

Example

The following command sets the Post-On delay for outlet .a5 to 90 seconds:

```
SLP: set outlet postondelay .a5 90<Enter>
```

Displaying outlet information

The Show Outlets command displays information about all outlets. This information includes:

- Sequencing and reboot timer values
- Descriptive outlet name, if applicable
- Outlet wakeup state and Post-On settings

To display outlet information:

3. At the SLP prompt, type `show outlets` and press **Enter**.

Example

The following command displays all outlet information:

```
SLP: show outlets<Enter>
Outlet   Outlet                          Wakeup  Post-On
ID       Name                            State   Delay seconds)

.A1      TowerA_Outlet1                  On      0
.A2      TowerA_Outlet2                  On      0
.A3      TowerA_Outlet3                  On      0
.A4      TowerA_Outlet4                  On      0
.A5      TowerA_Outlet5                  On      90
.A6      TowerA_Outlet6                  On      0
.A7      TowerA_Outlet7                  On      0
.A8      TowerA_Outlet8                  On      0
.A9      TowerA_Outlet9                  On      0
.A10     TowerA_Outlet10                 On      0
.A11     TowerA_Outlet11                 On      0
.A12     TowerA_Outlet12                 On      0
.A13     TowerA_Outlet13                 On      0
.A14     TowerA_Outlet14                 On      0
.A15     TowerA_Outlet15                 On      0
.A16     TowerA_Outlet16                 On      0
More (Y/es N/o):
Outlet Options:
Sequence Interval:  2 seconds
Reboot Delay:      15 seconds
```

Group Administration

Creating a group name

The Create Group command creates a new group name.

To create a group name:

3. At the command prompt, type `create group`, optionally followed by a descriptive name of up to 24 alphanumeric and other typeable characters (ASCII 33 to 126 decimal); spaces are not allowed; group names are not case sensitive. Press **Enter**.

Example

The following command creates a group named ServerGroup_1:

```
SLP: create group ServerGroup_1<Enter>
```

Removing a group name

The Remove Group command removes a group name.

To remove a group name:

4. At the command prompt, type `remove group`, optionally followed by a username. Press **Enter**.

Example

The following command removes group name ServerGroup_1:

```
SLP: remove group ServerGroup_1<Enter>
```

Adding an outlet to a group

The Add OutletToGroup command adds an outlet to a group. To add more than one outlet, but not all outlets, you must use multiple Add OutletToGroup commands.

To add an outlet to a group:

1. At the command prompt, type `add outlettogroup`, optionally followed by an outlet name and group name. Press **Enter**, or
2. Type `add OutletToGroup`, followed by all and the group name. Press **Enter**.

Examples

The following commands uses absolute outlet names to add outlets A1 and A2 to group name ServerGroup_1:

```
SLP: add OutletToGroup .a1 ServerGroup_1<Enter>
SLP: add OutletToGroup .a2 ServerGroup_1<Enter>
```

The following commands use the outlets' descriptive names to add outlets DataServer_1 and WebServer_1 to group name ServerGroup_1:

```
SLP: add OutletToGroup DataServer_1 ServerGroup_1<Enter>
SLP: add OutletToGroup WebServer_1 ServerGroup_1<Enter>
```

The following command adds all outlets to group name ServerGroup_1:

```
SLP: add OutletToGroup<Enter>
Outletname: all<Enter>
Groupname: ServerGroup_1<Enter>
```

Deleting an outlet from a group

The Delete OutletFromGroup command deletes an outlet from a group. To delete more than one outlet, but not all outlets, you must use multiple Delete OutletToGroup commands.

To delete an outlet from a group:

1. At the command prompt, type `delete outletfromgroup`, optionally followed by an outlet name and a group name. Press **Enter**, or
2. Type `delete outletfromgroup`, followed by all then the group name. Press **Enter**.

Outlet Administration

Creating a descriptive outlet name

The Set Outlet Name command assigns a descriptive name to an outlet. You may use this name in commands that require an outlet name as an alternative to using the outlet's absolute name.

To create an outlet name:

1. At the command prompt, type `set outlet name`, followed by the absolute outlet name and a descriptive name of up to 24 alphanumeric and other typeable characters (ASCII 33 to 126 decimal - spaces are not allowed). Outlet names are not case sensitive. Press **Enter**.

Example

The following command adds the descriptive name DataServer_1 to outlet .a1:

```
SLP: set outlet name .a1 DataServer_1<Enter>
```

Setting the outlet wakeup state

The Set Outlet Wakeup command set the default wakeup state for that outlet. In the event of a system-wide power loss, this state will be applied to the outlet when power is restored.

The wakeup state may be set to On, Off, or Last. Upon restoration of system power; If set to On, the unit will apply power to that outlet. If set to Off, the unit will not apply power to that outlet.

To set the wakeup state:

1. At the command prompt, type `set outlet wakeup`, followed by `on` or `off` and the outlet name. Press **Enter**.

Example

The following command sets the wakeup state for outlet .a1 to off:

```
SLP: set outlet wakeup off .a1<Enter>
```

Displaying outlet information

The Show Outlets command displays information about all outlets. This information includes:

- Descriptive outlet name, if applicable
- Outlet wakeup state setting

To display outlet information:

1. At the command prompt, type `show outlets` and press **Enter**.

Example

The following command displays all outlet information:

```
SLP: show outlets<Enter>
             Outlet   Outlet              Wakeup
             ID       Name                State
             .A1      DataServer_1        off
             .A2      WebServer_1         on
             .A3      FileServer_1        on
             .A4                          on
             .A5                          on
             .A6                          on
             .A7                          on
             .A8                          on
             .A9                          on
             .A10                         on
             .A11                         on
             .A12                         on
             .A13                         on
             .A14                         on
             .A15                         on
```

```
.A16                                on
More (Y/es N/o):
```

Serial Port Administration

Creating a descriptive serial port name

The Set Port Name command assigns a descriptive name to a serial port. You may use this name in commands that require a port name as an alternative to using the port's absolute name.

To create a port name:

1. At the command prompt, type `set port name`, followed by the absolute outlet name and a descriptive name of up to 24 alphanumeric and other typeable characters (ASCII 33 to 126 decimal - spaces are not allowed). Port names are not case sensitive.
2. Press **Enter**.

Note: *Port names '1' thru '64' and 'CONSOLE' are reserved system names and may not be used.*

Example

The following command adds the descriptive name Rack1 to Modem port:

```
SLP: set port name modem Rack1<Enter>
```

Setting the serial ports data rate

The Set Port Dsrchk command enables or disables active signal checking for serial/Pass-Thru connections to devices attached to any of the available serial ports.

Valid data rates are 1200, 2400, 4800, 9600, 19200, 38400, and 57600, 115200.

To set the serial port data rate:

1. At the command prompt, type `set port speed all`, followed by the data rate and press **Enter**.

Example

The following command sets the serial port data rate to 38400 BPS:

```
SLP: set port speed all 38400<Enter>
```

Enabling or disabling active signal checking for serial connections

The Set Port Speed Dsrchk command enables or disables active signal checking for serial connections to devices attached to any of the available serial ports.

To enable or disable active signal checking for serial connections:

1. At the command prompt, type **`set port dsrchk console, on or off,`** and press **Enter**.

Setting the serial port timeout value

The Set Port Speed Timeout command is used to set the serial port inactivity timeout period. The timeout period defines the maximum period of inactivity before automatically closing the session. The valid range for the period parameter is 0 to 5 (in minutes). The default period is 5.

Note: *Setting the timeout to '0' disables the timer.*

To set the serial port timeout value:

1. At the command prompt, type **`set port timeout,`** followed by a value from 0 to 5 (in minutes) and press **Enter**.

Displaying serial port information

The Show Ports command displays information about all serial port. This information includes:

- Serial port data rate
- Descriptive port name, if applicable
- DSR signal checking settings

To display serial port information:

1. At the command prompt, type **`show ports`** and press **Enter**.

Example

The following command displays all serial port information:

```
SLP: show ports<Enter>
  Serial Port Configuration
      ALL Ports:
      Baud rate: 38400           Connection Timeout: 5 minutes
      Port ID: Console           Port name: CONSOLE
           DSR Check: ON
      Port ID: Modem             Port Name: MODEM
           DSR Check: ON
         Initializations: ON
           Init String 2:   AT
           Init String 2:   AT E0 Q1 S0=1 S2=64 S12=50 &C1 &D2
           Attention String: @@@
```

System Administration

Creating a pre-login banner

The Set Banner command specifies text that appears prior to the login authentication. This feature allows administrators to configure a message up to 2070 characters for display of legal, disclaimer or other text as required by application. If left blank, the user will be taken directly to the login prompt.

Note: *For SSH sessions, the 'keyboard interactive' authentication method must be used for the banner to display.*

To create a pre-login banner:

2. At the command prompt, type **`set banner`** and press **Enter**. Type the desired pre-login banner text and when finished type Ctrl-z.

Creating a location description

The Set Location command specifies text that appears in the web browser control screen's Location field. The text is also appended to a "Welcome to" banner that appears when a user successfully logs in serially or through a Telnet session.

If you do not issue this command, or if you issue this command without specifying any text, the control screen's Location field will be blank and no Welcome to banner will be displayed.

To create a location description:

3. At the command prompt, type `set location`, followed by a descriptive name of up to 24 alphanumeric and other typeable characters (ASCII 32 to 126 decimal - spaces are allowed). Press **Enter**.

   Omitting any characters after typing `set location` deletes any previously specified text.

Examples

The following command specifies Florida HQ as the descriptive location for the control screen and the login banner:

```
SLP: set location Florida HQ<Enter>
```

The following command deletes any previously specified location description:

```
SLP: set location<Enter>
```

In this case, the control screen's Location field will be blank, and no Welcome banner will be displayed after a successful login.

Displaying system configuration information

The Show System command displays all system configuration information.

- Firmware version
- NIC module serial number and MAC address
- Hardware revision code and Flash size
- Uptime since last system restart
- System location description

See *4: Advanced Operations* for more information on SNMP.

To display system configuration information:

1. At the command prompt, type `show system` and press **Enter**.

Example

```
System Information
F/W Version:   SecureLinx Power Manager Version x.xx
NIC S/N:       1600001
MAC Address:   00-80-a3-8b-00-0e
```

```
H/W Rev Code:  0
Flash Size:    1 MB
Uptime:        0 days 6 hours 14 minutes 1 second
Location:      Florida HQ
```

Setting the LED display orientation

The Set Option Display command is used to configure the Current LED(s) display orientation.

To set the LED display orientation:

1. At the command prompt, type **`set option display`**, followed by **normal** or **inverted** and press **Enter**.

Example

The following sets the LED display orientation to Inverted:

```
SLP: set option display inverted<Enter>
```

Note: *When set to Inverted, the load will be reported in whole ampere increments.*

Enabling or disabling strong passwords

The Set Option Strong Passwords command is used to enable or disable the requirements for strong passwords. When enabled, all new passwords must be a minimum of 8 character in length with a least one uppercase letter, one lowercase letter, one number and on special character.

To enable or disable strong passwords:

1. At the command prompt, type **`set option strong password`**, followed by **enabled** or **disabled** and press **Enter**.

Enabling or disabling the external configuration reset button

The Set Option Button command enables or disables the external configuration reset button. This feature can enhance system security by protecting the SLP configurations from being reset locally.

Note: *If this feature has been enabled and the administrative account username/password has been lost, then the SLP must be returned to the factory for no-warranty reset of the configuration.*

To enable or disable the configuration rest button:

1. At the command prompt, type **`set option button`**, followed by **enabled** or **disabled** and press **Enter**.

Enabling or disabling the 'more' prompt

The Set Option More command enables or disables the 'more' prompt for display of data larger that the terminal window.

To enable or disable 'more':

1. At the command prompt, type **`set option more`**, followed by **enabled** or **disabled** and press **Enter**.

Setting the temperature scale

The Set Option TempScale command sets the temperature scale that the SLP will report in.

To set the temperature scale:

1. At the command prompt, type **`set option tempscale`**, followed by **Celsius** or **Fahrenheit** and press **Enter**.

Displaying system options

The Show Option command displays all system option information.

To display system option information:

2. At the command prompt, type **`show options`** and press **Enter**.

Example

```
SLP: show options
System Options
      Display Orientation:                    NORMAL
      Strong Passwords:                       DISABLED
      Configuration Reset Button:             ENABLED
      More Prompt:                            ENABLED
      Temperature Scale:                      CELSIUS
```

Creating a descriptive unit name

The Set Unit Name command assigns a descriptive name to a unit. This descriptive name is displayed when the Show Traps command is issued. See *Displaying trap configuration information* on page 76 for more information on the Show Traps command.

To create a unit name:

3. At the command prompt, type `set unit name`, followed by the absolute unit name, then the descriptive name of up to 24 alphanumeric and other typeable characters (ASCII 33 to 126 decimal - spaces are not allowed).

4. Press **Enter**.

Examples

The following command adds the descriptive name Florida_HQ_1 to unit.a:

```
SLP: set unit name .a Florida_HQ_1<Enter>
```

Displaying unit information

The Show Units command displays information about the unit. This information includes the absolute and descriptive unit names.

To display unit information:

1. At the command prompt, type `show units` and press **Enter**.

Example

```
SLP: show units<Enter>
Unit   Unit
ID      Name
.A      Florida_HQ_1
```

Creating a descriptive infeed name

The Set Infeed Name command assigns a descriptive name to an infeed. This descriptive name is displayed when the Show Traps command is issued. See *Displaying trap configuration information* on page 76 for more information on the Show Traps command.

To create an infeed name:

1. At the command prompt, type `set infeed name`, followed by the absolute infeed name, then the descriptive name of up to 24 alphanumeric and other typeable characters (ASCII 33 to 126 decimal - spaces are not allowed).
2. Press **Enter**.

Example

The following command adds the descriptive name HQ_1_Infeed_A to the infeed on the unit:

```
SLP: set infeed name .aa HQ_1_Infeed_A<Enter>
```

Displaying Infeed information

The Show Infeeds command displays information about all infeeds. This information includes the absolute and descriptive infeed names.

To display unit information:

1. At the command prompt, type `show infeeds` and press **Enter**.

Example

```
SLP: show infeeds<Enter>
Input    Input
Feed ID  Feed Name
.AA      HQ_1_Infeed_A
```

Creating a descriptive tower name

The Set Tower Name command assigns a descriptive name to a tower. This descriptive name is displayed when the Show Traps command is issued. See *Displaying trap configuration information* on page 76 for more information on the Show Traps command.

To create a tower name:

3. At the command prompt, type **`set tower name`**, followed by the absolute tower name, then a descriptive name of up to 24 alphanumeric and other typeable characters (ASCII 33 to 126 decimal - spaces are not allowed). Press **Enter**.

Example

The following command adds the descriptive name Florida__HQ_1 to tower .a:

```
SLP: set tower name .a Florida_HQ_1<Enter>
```

Displaying Tower information

The Show Towers command displays information about the SLP. This information includes the absolute and descriptive SLP names.

To display unit information:

1. At the command prompt, type **`show towers`** and press **Enter**.

Example

```
SLP: show towers<Enter>
Tower    Tower
ID       Name
.A       Florida_HQ_1
```

Displaying the firmware version

The Version command displays the firmware version.

To display the firmware version:

1. At the command prompt, type `version` and press **Enter**.

Performing a warm boot

The Restart command performs a warm boot of the unit.

Note: *System user/outlet/group/port configuration or outlet states are NOT changed or reset with this command.*

To perform a warm boot:

1. At the command prompt, type `restart` and press **Enter**.

TCP/IP Administration

Note: *A restart of the unit is required after setting or changing any TCP/IP configurations*.

Enabling or disabling DHCP support

The Set DHCP command enables or disables DHCP support.

To enable or disable DHCP support:

1. At the command prompt, type `set dhcp`, followed by enabled or disabled and press **Enter**.

Setting the IP address

The Set Ipaddress command sets the TCP/IP address of the network interface controller.

To set the IP address:

1. At the command prompt, type `set ipaddress`, followed by the IP address and press **Enter**.

Example

The following command sets the IP address to 12.34.56.78:

```
SLP: set ipaddress 12.34.56.78<Enter>
```

Setting the subnet mask

The Set Subnet command sets the subnet mask for the network in which the unit will be attached.

To set the subnet mask:

1. At the command prompt, type `set subnet`, followed by the subnet mask and press **Enter**.

Example

The following command sets the subnet mask to 255.0.0.0

```
SLP: set subnet 255.0.0.0<Enter>
```

Setting the gateway

The Set Gateway command sets the IP address of the default gateway the unit uses to access external networks.

To set the gateway IP address:

1. At the command prompt, type `set gateway`, followed by the gateway IP address and press **Enter**.

Example

The following command sets the gateway IP address to 12.34.56.1:

```
SLP: set gateway 12.34.56.1<Enter>
```

Setting the DNS IP address

The Set DNS command sets the TCP/IP address of the Domain Name server (DNS).

To set the DNS IP address:

1. At the command prompt, type `set`, followed by **dns1** or **dns2** and the Domain Name server's IP address. Press **Enter**.

Example

The following command sets the primary Domain Name server IP address to 98.76.54.254:

```
SLP: set dns1 98.76.54.254<Enter>
```

Enabling or disabling automatic updates

The Set FTP Autoupdate command is used to enable or disable automatic firmware update support.

To enable or disable automatic updates:

1. At the command prompt, type `set ftp autoupdate`, followed by **enabled** or **disabled** and press **Enter**.

Setting the automatic update scheduled day

The Set FTP Autoupdate Day command is used to set the day when automatic updates occur.

To set the automatic update day:

1. At the command prompt, type `set ftp autoupdate day`, followed by the day of the week or everyday and press **Enter**.

Example

The following command sets the automatic update day to Sunday:

```
SLP: set ftp autoupdate day sunday<Enter>
```

Setting the automatic update scheduled hour

The Set FTP Autoupdate Hour command is used to set the hour of the day when automatic updates occur.

To set the automatic update hour:

1. At the command prompt, type `set ftp autoupdate hour`, followed by an hour of the day and press **Enter**.

Examples

The following command sets the automatic update hour to 12 AM:

```
SLP: set ftp autoupdate hour 12am<Enter>
```

The following command sets the automatic update hour to 3 PM:

```
SLP: set ftp autoupdate hour 3pm<Enter>
```

SNTP Administration

SLP supports the use of a network time service to provide a synchronized time reference.

Setting the SNTP server address

The Set SNTP command is used to set the primary and secondary SNTP server addresses.

To set the SNTP server address:

1. At the command prompt, type `set sntp`, followed by **primary** or **secondary** and the SNTP server IP address or hostname. Press **Enter**.

Examples

The following command sets the primary SNTP server address to 204.152.184.72:

```
SLP: set sntp primary 204.152.184.72<Enter>
```

The following command sets the secondary SNTP server address to cuckoo.nevada.edu:

```
SLP: set sntp secondary
cuckoo.nevada.edu<Enter>
```

Setting the local GMT offset

The Set SNTP GMT offset command is used to set the offset from GMT for the date/time returned by SNTP. The offset can be configured in whole hours between -12 and 12 hours.

Note: *The SLP does not support automatic adjustment for daylight savings*.

To set the local GMT offset:

1. At the command prompt, type `set sntp gmtoffset`, followed by the offset value and press **Enter**.

Example

The following command sets the local GMT offset to -12:

```
SLP: set sntp gmtoffset -12<Enter>
```

Displaying SNTP configuration information

The Show SNTP command displays all SNTP configuration information.

To display SNTP configuration information:

1. At the command prompt, type `show sntp` and press **Enter**.

Example

The following command displays the SNTP configuration information:

```
SLP: show sntp<Enter>
  Date/Time (Local GMT Offset -12): 2006-02-21 21:32:48
  Primary Host:   204.152.184.72
  Secondary Host: cuckoo.nevada.edu
```

Displaying network configuration information

The Show Network command displays TCP/IP, Telnet, SSH, Web, SSL and SNMP configuration information.

IP address, subnet mask and gateway

Enabled-disabled status of Telnet, SSH, HTTP,SSL and SNMP support

Telnet, SSH, and HTTP port numbers

HTTP authentication method and SSL access setting

Network status

See *4:Advanced Operations* for more information on SNMP

To display network configuration information:

2. At the command prompt, type `show network` and press **Enter**.

Example

The following command displays the network configuration information:

```
SLP: show network<Enter>
Network Configuration
       IP Address:   12.34.56.78
       Subnet Mask:  255.0.0.0
       Gateway:      12.34.56.1
        Telnet:      Enabled   Port: 23
        SSH:         Enabled   Port: 65535
        HTTP:        Enabled   Port: 80  Security: BASIC
        SSL:         Enabled             Access:  Required
        SNMP:        Enabled
Network Status
      Link:           Up
      Speed:          100 Mbps
      Duplex:         Full
      Negotiation:    Auto
```

HTTP Administration

Note: *A restart is required after setting or changing ANY Telnet/Web configurations. At the command prompt, type `restart` and press **Enter**.*

Enabling and disabling HTTP support

The Set HTTP command is used to enable or disable HTTP support.

To enable or disable HTTP support:

1. At the command prompt, type `set http`, followed by `enabled` or `disabled` and press **Enter**.

Changing the HTTP server port

With HTTP support enabled, the HTTP server watches and responds to requests on the default HTTP port number 80. This port number may be changed using the Set HTTP Port command.

To change the HTTP port:

1. At the command prompt, type `set http port`, followed by the port number and press **Enter**.

Example

The following changes the HTTP port number to 2048:

```
SLP: set HTTP port 2048<Enter>
```

Setting the HTTP authentication method

The Set HTTP Security command is used to set the method of authentication. The HTTP server supports two authentication methods for security and validation of the username-password – Basic and MD5 digest.

To set the HTTP authentication method:

1. At the command prompt, type `set http security`, followed by `basic` or `md5` and press **Enter**.

Telnet Administration

Note: *A restart of the unit is required after setting or changing ANY Telnet/Web configurations. See Performing a warm boot on page 57 for more information.*

Enabling and disabling Telnet support

The Set Telnet command is used to enable or disable Telnet support.

To enable or disable Telnet support:

1. At the command prompt, type `set Telnet`, followed by `enabled` or `disabled` and press **Enter**.

Changing the Telnet port

With Telnet support enabled, the Telnet server watches and responds to requests on the default Telnet port number 23. This port number may be changed using the Set Telnet Port command.

To change the Telnet socket:

1. At the command prompt, type `set Telnet port`, followed by the port number and press **Enter**.

Example

The following changes the Telnet port number to 7001:

```
SLP: set Telnet port 7001<Enter>
```

FTP Administration

You may install new versions of firmware using File Transfer Protocol (FTP). This allows access to new firmware releases for firmware improvements and new feature additions. The following commands are used to configure the unit for an FTP firmware upload. See *Uploading Firmware* for more information on initiating a FTP firmware upload.

Setting the FTP Host IP address

The Set FTP Host command sets the FTP host IP address allowing for firmware file uploads.

To set the FTP Host IP address:

1. At the command prompt, type `set ftp host`, followed by the Host IP address and press **Enter**.

Example

The following command sets the FTP Host IP address to 12.34.56.99:

```
SLP: set ftp host 12.34.56.99<Enter>
```

Setting the FTP username

The FTP Username command sets the username as required by the FTP Host.

To set the FTP username:

1. At the command prompt, type `set ftp username`, followed by the FTP username and press **Enter**.

Example

The following command sets the FTP username to Guest:

```
SLP: set ftp username guest<Enter>
```

Setting the FTP Password

The FTP Password command sets the password as required by the FTP Host.

To set the FTP password:

1. At the command prompt, type `set ftp password`, followed by the FTP password and press **Enter**.

Example

The following command sets the FTP password to OpenSesame:

```
SLP: set ftp password OpenSesame<Enter>
```

Setting the filename to be uploaded

The FTP Filename command sets the filename of the firmware file to be uploaded.

To set the FTP filename:

1. At the command prompt, type `set ftp filename`, followed by the firmware filename and press **Enter**.

Example

The following command sets the FTP filename to snb_s50a.bin:

```
SLP: set ftp filename snb_s50a.bin<Enter>
```

Setting the file path for the file to be uploaded

The FTP Filepath command sets the file path for the firmware file to be uploaded.

To set the FTP file path:

1. At the command prompt, type `set ftp filepath`, followed by the filepath and press **Enter**.

Example

The following command sets the FTP file path to ftp:// slp:

```
SLP: set ftp filepath ftp://slp<Enter>
```

Displaying FTP configuration information

The Show FTP command displays all FTP configuration information.

FTP Host IP address

FTP Host username and password

Firmware file path and filename

To display FTP configuration information:

1. At the command prompt, type `show ftp` and press **Enter**.

Example

The following command displays the FTP configuration information:

```
SLP: show ftp<Enter>
       FTP Configuration
              Host IP Address: 12.34.56.99
              Username:        guest
              Password:        OpenSesame
              Directory:       ftp://slp
              Filename:        SLP_xxxx.bin
```

4: Advanced Operations

SSL

Secure Socket Layers (SSL) version 3 enables secure web browser sessions between a Remote Power Manager and a remote user. SSL provides two chief features designed to make TCP/IP (Internet) transmitted data more secure:

- Authentication – The connecting client is assured of the identity of the server.
- Encryption – All data transmitted between the client and the server is encrypted rendering any intercepted data unintelligible to any third party.

SSL uses the public-and-private key encryption system by RSA, which also requires the use of digital certificates. An SSL Certificate is an electronic file uniquely identifying individuals or websites and enables encrypted communication; SSL Certificates serve as a kind of digital passport or credential. The product's SSL Certificate enables the client to verify the unit's authenticity and to communicate with the unit securely via an encrypted session, protecting confidential information from interception and hacking.

Table 4-1. SSL Command Summary

Command	Description
Set SSL	Enables/disables SSL support
Set SSL access	Sets SSL access as optional or required

Enabling and Setting up SSL Support

Note: *A restart of the unit is required after setting or changing ANY SSL configurations. See Performing a warm boot on page 57 for more information.*

Enabling or disabling SSL support

The Set SSL command is used to enable or disable SSL support.

To enable or disable SSL support:

1. At the command prompt, type `set ssl`, followed by `enabled` or `disabled` and press **Enter**.

Setting SSL access level

The Set SSL Access command is used to assign use of SSL as optional or required. The default access level is set to optional.

To change the access level:

1. At the command prompt, type `set ssl access`, followed by `optional` or `required`, and press **Enter**.

Example

The following changes the access level to required:

```
SLP: set ssl access required<Enter>
```

SSL Technical Specifications

Secure Socket Layer (SSL) version 3

Transport Layer Security (TLS) version 1 (RFC 2246)

SSL/TLS-enabled HTTPS server (RFC 2818)

Self-Signed X.509 Certificate version 3 (RFC 2459)

Asymmetric Cryptography:

- 1024-bit RSA Key Exchange

Symmetric Cryptography Ciphers:

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_DES_CBC_SHA

SSH

Secure Shell (SSH) version 2 enables secure network terminal sessions between a Remote Power Manager and a remote user over insecure network. SSH provides an encrypted terminal session with strong authentication of both the server and client, using public-key cryptography and is typically used as a replacement for unencrypted Telnet. In addition to enabling secure network terminal sessions to the unit for configuration and power management, the SSH session may be used for secure Pass-Thru connections to attached devices.

SSH requires the configuration and use of a client agent on the client PC. There are many freeware, shareware or for-purchase SSH clients available. Two examples are the freeware client PuTTY and the for-purchase client SecureCRT by VanDyke Software. For configuration and use of these clients, please refer to the applicable software documentation.

Table 4-2. SSH Command Summary

Command	Description
Set SSH	Enables/disables SSH support
Set SSH port	Sets the SSH server port number

Enabling and Setting up SSH Support

Note: *A restart of the unit is required after setting or changing ANY SSH configurations. See Performing a warm boot on page 57 for more information.*

Enabling or disabling SSH support

The Set SSH command is used to enable or disable SSH support.

To enable or disable SSH support:

1. At the command prompt, type `set ssh`, followed by `enabled` or `disabled` and press **Enter**.

Changing the SSH server port

With SSH support enabled, the SSH server watches and responds to requests on the default SSH port number 22. This port number may be changed using the Set SSH Port command.

To change the SSH port:

1. At the command prompt, type `set ssh port`, followed by the port number and press **Enter**.

Example

The following changes the SSH port number to 65535:

```
SLP: set ssh port 65535<Enter>
```

SSH Technical Specifications

Secure Shell (SSH) version 2

Asymmetric Cryptography:

Diffie-Hellman DSA/DSS 512-1024 (random) bits per NIST specification

Symmetric Cryptography:

AES256-CBC	RIJNDAEL256-CBC	3DES-192-CBC
AES192-CBC	RIJNDAEL192-CBC	BLOWFISH-128-CBC
AES128-CBC	RIJNDAEL128-CBC	ARCFOUR-128

Message Integrity:

HMAC-SHA1-160 HMAC-SHA1-96

HMAC-MD5-128 HMAC-MD5-96

Authentication:

Username/Password

Session Channel Break Extension (for RS-232 Break)

SNMP

The SLP family of products supports the Simple Network Management Protocol (SNMP). This allows network management systems to use SNMP requests to retrieve information and control power for the individual outlets.

The SNMP implementation includes an SNMP v1 agent supporting standard MIB I and MIB II objects. A private enterprise MIB extension is also supported to provide remote power control.

Note: *For security, SNMP support is disabled by default*.

Table 4-3. SNMP Command Summary

Command	Description
Set snmp	Enables or disables SNMP support
Set snmp getcomm	Sets the 'get' community string
Set snmp setcomm	Sets the 'set' community string
Set snmp trapdest1	Sets a destination IP addresses for traps
Set snmp trapdest2	Sets a destination IP addresses for traps
Set snmp traptime	Sets the delay for steady state condition traps
Show snmp	Displays all SNMP configuration information

Enabling and Setting up SNMP Support

SNMP support must be enabled and configured for access to private enterprise MIB extensions for remote power control, and for generation of all SNMP traps.

Enabling/disabling SNMP support

The SNMP command is used to enable or disable SNMP support.

To enable SNMP support:

1. At the command prompt, type `set snmp`, followed by `enabled` or `disabled` and press **Enter**.

Note: *A restart is required after enabling or disabling SNMP support. See* *Performing a warm boot on page 57* *for more information*.

Setting trap destinations

The Set SNMP Trapdest1 and Trapdest2 commands are used to set the IP addresses of SNMP management stations receiving all traps. A maximum of two trap destinations are supported; one must be defined to enable trap generation.

To set the trap destination:

1. At the command prompt, type `set snmp`, `trapdest1` or `trapdest2`, the Ipaddress and press **Enter**.

Examples

The following sets the trap destination 1 to 64.42.31.208:

```
SLP: set snmp trapdest1 64.42.31.208<Enter>
```

The following sets the trap destination 2 to snmp.lantronix.com:

```
SLP: set snmp trapdest2 snmp.lantronix.com
<Enter>
```

To reset the trap destination:

1. At the command prompt, type `set snmp`, `trapdest1` or `trapdest2`, `0.0.0.0` and press **Enter**.

Setting the trap timer

The Set Traptime command sets the timer period between repeated error-condition traps. The valid range for the timer period is 1 to 65535 (in seconds).

The default value for the timer period is 60 seconds.

To set the trap timer:

1. At the command prompt, type set `traptime`, followed by the timer period and press **Enter**.

Example

The following sets the timer period to 180 seconds:

```
SLP: set traptime 180<Enter>
```

Setting the Get/Set community strings

Two SNMP community strings provide varying levels of access to objects defined in the private enterprise MIB extensions.

Community strings may be 1 to 24 characters.

Setcomm

The Setcomm string provides read-write access to private enterprise MIB objects.

The default Setcomm string is “private”

To set the Setcomm community string:

1. At the command prompt, type set `snmp setcomm`, followed by the string and press **Enter**.

Getcomm

The Getcomm string provides read-only access to private enterprise MIB objects. The default Getcomm string is “public”.

To set the Getcomm community string:

1. At the command prompt, type `set snmp getcomm`, followed by the string and press **Enter**.

Setting SNMP IP Restrictions

The Set SNMP IP Restrictions command supports SNMP Manager GET and SET requests to only be allowed from the IP addresses of the defined traps destinations.

To set SNMP IP Restrictions:

1. At the command prompt, type set `snmp iprestrict trapdests` and press **Enter**.

To remove SNMP IP Restrictions:

1. At the command prompt, type set `snmp iprestrict none` and press **Enter**.

Setting the SNMP SysName

The Set SNMP SysName command is used to set the SNMP MIB-II SysName object.

To set the SysName object:

1. At the command prompt, type `snmp sysname`, followed by the object name and press **Enter**.

Setting the SNMP SysLocation

The Set SNMP SysLocation command is used to set the SNMP MIB-II SysLocation object.

To set the SysLocation object:

1. At the command prompt, type `snmp syslocation`, followed by the object location and press **Enter**.

Setting the SNMP SysContact

The Set SNMP SysContact command is used to set the SNMP MIB-II SysContact object.

To set the SysContact object:

1. At the command prompt, type `snmp syscontact`, followed by the object contact and press **Enter**.

Setting the Trap community string

The Set SNMP Trapcomm command is used to set the community string that is included with all generated traps. This string must be defined to enable trap generation.

The trap community string may be 1 to 24 characters. The default Trapcomm string is “trap”.

To set the Trapcomm community string:

1. At the command prompt, type set `snmp trapcomm`, followed by the string and press **Enter**.

Displaying SNMP configuration information

The Show SNMP command displays all SNMP configuration information.

SNMP support status

SNMP community strings

Trap timer value

Trap destinations

To display SNMP configuration information:

1. At the command prompt, type show snmp and press **Enter**.

Example

The following command displays the SNMP configuration information:

```
SLP: show snmp<Enter>
   SNMP Configuration
      SNMP:                                Enabled
      SET Community String:                private
      GET Community String:                public
      TRAP Community String:               trap
      Error Trap Repeat Time (seconds):    180
      Trap Destination 1:                  64.42.31.208
      Trap Destination 2:             snmp.lantronix.com
      IP Restrictions:             Trap Destinations Only
      SysName:                     No Name
      SysLocation                  No Location
      SysContact                   No Contact
```

SNMP Traps

Three types of SNMP traps are supported. Traps are enabled at the unit (T), infeed (I) or outlet (O) level.

Table 4-4. Trap Summary

Name	Level(s)	Description
Status	T, I, O	Operational status change
Change	O	Control status change
Load	I	Input load out of limit

All traps include the Location of the unit as defined with the Set Location command. See *Creating a pre-login banner*

The Set Banner command specifies text that appears prior to the login authentication. This feature allows administrators to configure a message up to 2070 characters for display of legal, disclaimer or other text as required by application. If left blank, the user will be taken directly to the login prompt.

Note: *For SSH sessions, the 'keyboard interactive' authentication method must be used for the banner to display.*

To create a pre-login banner:

4. At the command prompt, type **`set banner`** and press **Enter.** Type the desired pre-login banner text and when finished type Ctrl-z.

Creating a location description on page 5252 for more information.

Status trap

A Status trap is generated when an error condition occurs on a unit, infeed or outlet. Status traps include the reported Status, the Location of the unit, and identifier and name of the affected unit, infeed or outlet.

Any Trap Status generates a Status trap and triggers the trap timer. A new trap is generated at the end of every timer period until the Status returns to a non-error status.

Table 4-5. Unit Status Traps

Status	Error	Description
Normal		Unit is working correctly
NoComm	x	Communication to the unit has been lost
Status	Error	Description

Table 4-6. Infeed Status Traps

Status	Error	Description
On		Infeed is on
OffError	x	Infeed should be on but no current is sensed at the infeed
NoComm	x	Communication to the infeed has been lost

Table 4-7. Outlet Status Traps

Status	Error	Description
On		Outlet is on
Off		Outlet is off
OnWait		Outlet Status in transition
OffWait		Outlet Status in transition
OnError	x	Outlet should be off but current is sensed at the outlet
OffError	x	Outlet should be on but no current is sensed at the outlet
OffFuse	x	Outlet should be on but a blown fuse has been detected
NoComm	x	Communication to the outlet has been lost

Note: *Traps are generated according to a hierarchical architecture; i.e. if a Unit Status enters a trap condition, only the Unit Status trap is generated. Infeed and Outlet Status traps are suppressed until the Unit Status returns to Normal*.

Change trap

The Change trap is generated for all outlet status changes between any on/off conditions. Change traps include the outlet status, Location of the unit, and identifier and name of the affected outlet. For descriptions of the outlet status types, please refer to the prior table.

Load Trap

The Load trap is generated whenever the total input load on an infeed exceeds a preset threshold. Load traps include the reported input load, load status, Location of the unit, and identifier and name of the affected infeed.

Any error state generates a Load trap and triggers the trap timer. A new trap is generated at the end of every timer period until the Load returns to a non-error status.

Table 4-8. Load Traps

Status	Error	Description
Normal		Infeed is on and within preset thresholds
NotOn		Infeed is off
Reading		Non-error state – Load status currently being read
LoadHigh	x	Infeed current load exceeds preset threshold
OverLoad	x	Infeed current load exceeds the measurable range for the infeed
ReadError	x	Unable to read Load status
NoComm	x	Communication to the infeed

Configuring Traps

Table 4-9. SNMP Trap Command Summary

Command	Description
Set Trap Unit Status	Enables or disables the Unit Status trap
Set Trap Infeed Status	Enables or disables the Infeed Status trap off
Set Trap Infeed Load	Enables or disables the Infeed Load trap
Set Trap Infeed HighThresh	Sets the Infeed Load trap high limit
Set Trap Outlet Change	Enables or disables the Outlet Change trap
Set Trap Outlet Status	Enables or disables the Outlet Status trap
Show Traps	Displays trap configurations

Enabling or Disabling a Status trap

The Set Trap <infeed|outfeed|outlet> Status command is used to enable or disable Status traps for a Unit, Infeed or Outlet.

To Enable or Disable a Status trap:

1. At the command prompt, type `set trap` (`unit`, `infeed` or `outlet`) `status`, followed by the tower, infeed or outlet name, and `on` or `off`. Press **Enter**, or
2. Type `set trap` (`unit`, `infeed` or `outlet`) `Status all`, followed by `on` or `off` and press **Enter**.

Examples

The following command enables the Status trap using the unit's absolute name:

```
SLP: set trap unit status .a on<Enter>
```

The following command enables the Status trap for the unit named Florida_HQ_1:

```
SLP: set trap unit status Florida_HQ_1 on<Enter>
```

Note: *Enabling lower hierarchical traps automatically enables traps of higher hierarchical value: i.e. enabling an Outlet Status trap automatically enables the Infeed and Unit Status traps for that outlet. Conversely, if a Unit Status trap is disabled, all associated Infeed Status & Load and Outlet Status traps will be disabled.*

Enabling or Disabling a Load trap

The Set Trap Infeed Load command is used to enable or disable an Infeed Load trap.

To Enable or Disable a Load trap:

1. At the command prompt, type `set trap infeed load`, followed by the infeed name, and `on` or `off`. Press **Enter**, or
2. Type `set trap infeed load all`, followed by `on` or `off` and press **Enter**.

Examples

The following command enables the Load trap using the unit's absolute name:

```
SLP:  set trap infeed load.aa on<Enter>
```

The following command disables the Load trap:

```
SLP:  set trap infeed load all off<Enter>
```

Note: *Enabling lower hierarchical traps automatically enables traps of higher hierarchical value: i.e. enabling an Infeed Load trap automatically enables the Infeed and Unit Status traps for that infeed*.

Setting the Infeed Load limit

The Set Trap Infeed Loadhigh command is used to set the upper load limits for an input feed.

To set the infeed load limit:

1. At the command prompt, type `set trap infeed loadhigh`, followed by the infeed name, and a value from 0 to 255 in amperes. Press **Enter**.

Example

The following command sets the infeed load limit for the infeed to 25 amperes, using the infeed's absolute name:

```
SLP:  set trap infeed loadhigh.aa 25<Enter>
```

Enabling or Disabling a Change trap

The Set Trap Outlet Change command is used to enable or disable an Outlet Change trap.

To Enable or Disable a Change trap:

4. At the command prompt, type `set trap outlet change`, followed by the outlet name and `on` or `off`. Press **Enter**, or

5. Type `set trap outlet change all`, followed by `on` or `off` and press **Enter**.

Example

The following command enables the Change trap for the third outlet using the outlet's absolute name:

```
SLP:  set trap outlet change .a3 on<Enter>
```

Displaying trap configuration information

The Show Traps command displays information about all traps.

To display trap information:

1. At the command prompt, type `show traps` and press **Enter**.

Example

The following command requests trap configuration information:

```
SLP:  show traps <Enter>
Unit trap configuration:
   Unit    Unit                 Status
   ID       Name                  Trap
   .A       Florida_HQ_1          ON
   More (Y/es N/o): y
Input feed trap configuration:
   Input    Input                 Status   Load     High
   Feed ID  Feed Name             Trap     Trap   Thresh
   .AA      HQ_1_Infeed_A         ON       ON      255 A
   More (Y/es N/o): y
Outlet trap configuration:
   Outlet   Outlet                Change   Status
   ID       Name                  Trap     Trap
   .AA1     DataServer_1          OFF      ON
   .AA2     WebServer_1           OFF      ON
   .AA3     FileServer_1          OFF      ON
   .AA4                           OFF      ON
   .AA5                           OFF      ON
   .AA6                           OFF      ON
   .AA7                           OFF      ON
   .AA8                           OFF      ON
   More (Y/es N/o): y.
```

LDAP

The SLP family of product supports Lightweight Directory Access Protocol (LDAP) version 3. This support enables authentication with LDAP servers; user accounts do not need to be individually created locally on each SLP device.

This allows administrators to pre-define and configure (in each SLP product and in the LDAP server) a set of necessary LDAP Groups, and access rights for each. User's access rights can then be assigned or revoked simply by making the user a member of one-or-more pre-defined SLP LDAP Groups. User accounts can be added, deleted, or changed in the LDAP server without any changes needed on individual SLP products.

SLP LDAP support has been tested in the following environments:

- Microsoft Active Directory (MSAD)
- Novell eDirectory (eDir)
- OpenLDAP

LDAP Command Summary

Command	Description
Set Authororder	Specifies the authentication order for each new session attempt
Set LDAP	Enables/disables LDAP support
Set LDAP Host	Sets the IP address or hostname of the Directory Services server
Set LDAP Port	Sets the LDAP server port number
Set LDAP Bind	Specifies the LDAP bind request password type
Set LDAP BindDN	Specifies the user account Fully-Qualified Distinguished Name (FQDN) for binds
Set LDAP BindPW	Specifies the user account password for binds
Set LDAP GroupAttr	Specifies the user class distinguished name (DN) or names of groups a user is a member of
Set LDAP GroupType	Specifies the data type for the Set LDAP GroupAttr command
Set LDAP UseTLS	Enables/disables LDAP over TLS/SSL support
Set LDAP UserBaseDN	Sets the base distinguished name (DN) for the username search at login
Show LDAP	Displays LDAP configurations
Set DNS	Sets the IP address of the Domain Name server
Ping	Verifies proper DNS configuration by name resolution
Show Network	Displays network configuration information
Create LDAPGroup	Adds and LDAP group name
Remove LDAPGroup	Deletes an LDAP group name
Add GrouptoLDAP	Grants an LDAP group access to one or more groups
Add OutlettoLDAP	Removes access to one or more outlets for an LDAP group

Add PorttoLDAP	Grants an LDAP group access to one or more serial ports
Delete GroupfromLDAP	Removes access to one or more groups for an LDAP group
Delete OutlettoLDAP	Removes access to one or more outlets for an LDAP group
Delete PortfromLDAP	Removes access to one or more serial ports for an LDAP group
Set LDAPGroup Access	Sets the access level for an LDAP group
Set LDAPGroup Envmon	Grants or removes privileges to view input and environmental monitoring status
List LDAPGroup	Displays all accessible outlets/groups/ports for an LDAP group

Enabling and Setting up LDAP Support

There are a few configuration requirements for properly enabling and setting up LDAP support. Below is an overview of the maximum requirements.

Directory Services server configuration requirements:

1. Define at least on LDAP group.
2. Assign users to the LDAP group.

SLP configuration requirements:

1. Enable LDAP support.
2. Define the IP address and domain component of at least one Directory Services server.
3. Set the LDAP bind request method being utilized by the Directory Services server.
4. Define the IP address of at least on DNS server.
5. Test DNS server configuration using SLP 'ping' support.
6. Define at least one LDAP group and assign access rights for that group.

Note: *LDAP group names on the Directory Service server and the SLP must match*.

Enabling and disabling LDAP Support

The Set LDAP command is used to enable or disable LDAP support.

To enable or disable LDAP support:

1. At the command prompt, type **`set ldap`**, followed by **enabled** or **disabled** and press **Enter**.

Setting the LDAP host address

The Set LDAP Host command sets the TCP/IP address of the Directory Services server.

To set the LDAP host address:

1. At the command prompt, type **`set ldap`**, followed by **host1** or **host2** and the Directory Services server's IP address or hostname. Press **Enter**.

Examples

The following command sets the primary Directory Services server IP address to 98.76.54.32:

```
SLP:  set ldap host1 98.76.54.32<Enter>
```

The following command disables the Load trap:

```
SLP:  set ldap host2 ldap.ltrx.com<Enter>
```

Changing the LDAP server port

The Set LDAP port command sets the port to which the SLP sends LDAP requests to the previously defined LDAP server. The default port is 389.

To change the LDAP server port:

1. At the command prompt, type **`ldap port`**, followed by the port number and press **Enter**.

Example

The following command sets the LDAP port server number to 8888:

```
SLP:  set ldap port 8888<Enter>
```

Enabling and disabling LDAP over TLS/SSL support

The Set LDAP UseTLS command is used to enable or disable LDAP over TLS/SSL support.

To enable or disable LDAP over TLS/SSL support:

1. At the command prompt, type **`ldap usetls`**, followed by **yes** or **no** and press **Enter**.

Example

The following command sets the LDAP port server number to 8888:

```
SLP:  set ldap port 8888<Enter>
```

Note: *If LDAP over TLS/SSL is enabled, MD5 binding is disabled.*

Setting the LDAP bind password type

The Set LDAP Bind command sets the password type used in the bind request. The SLP supports two LDAP bind methods – Simple and MD5.

The Simple method utilizes unencrypted delivery of a username-password over the network to the Active Directory server for authentication

The MD5 digest method provides much stronger protection utilizing one-way encoded hash numbers, never placing the username-password on the network. For more information on MD5, see Setting the HTTP authentication method on page 61.

Note: *Windows 2000 is known only to support Simple binding. Windows 2003 supports both Simple and MD5 binding.*

To set the bind password type:

1. At the command prompt, type **`ldap bind`**, followed by **simple** or **md5** and press **Enter**.

Note: *If MD5 binding is enabled, LDAP over TLS/SSL is disabled.*

Setting the search bind Distinguished Name (DN):

The Set LDAP BindDN command is used to set the fully-qualified distinguished name (FQDN) for user accounts to bind with. This is required for directory services that do not support anonymous bind.
This field is used ONLY with Simple Binds.
Maximum string length is 124 characters.

Note: *If left blank, an anonymous bind will be attempted. This field is used ONLY with Simple binds.*

To set the search bind DN:

1. At the command prompt, type **`ldap binddn`**, and press **Enter**. At the following prompt, type the FQDN and press **Enter**.

Example

The following sets the FQDN for MSAD to 'cn=guest, cn=Users, dc=lantronix, dc=com':

```
SLP:  set ldap binddn<Enter>
Enter Search Bind DN (Max characters 124):
cn=guest, cn=Users, dc=lantronix, dc=com
```

Setting the search bind Distinguished Name (DN) password:

The Set LDAP BindPW command is used to set the password for the user account specified in the Search Bind DN.
Maximum password size is 20 characters.

To set the search bind DN:

2. At the command prompt, type **`ldap bindpw`**, and press **Enter**. At the following prompt, type the bind password and press **Enter**.

Setting the group membership Attribute:

The Set LDAP GroupAttr command is used to specify the name of user class attributes that list distinguished names (DN), or names of groups that a user is a member of. Maximum string length is 30 characters.

To set the Group Membership Attribute:

1. At the command prompt, type **`ldap groupattr`**, and press **Enter**. At the following prompt, type the group membership attribute and press **Enter**.

Example

The following sets the group membership attribute for MSAD to 'memberof':

```
SLP:  set ldap groupattr<Enter>
Enter Group Member Attr (Max characters 30):
```

```
Memberof<Enter>
```

Setting the group membership value type:

The Set LDAP GroupType command is used to specify whether the values of group Membership Attribute represent the Distinguished Name (DN) of a group or just the name of the group.

To set the group membership value type:

2. At the command prompt, type **`ldap grouptype`**, followed by DN or Name and press **Enter**.

Example

The following sets the group membership attribute for MSAD to 'memberof':

```
SLP:  set ldap grouptype DN<Enter>
```

Setting the user search base Distinguished Name (DN):

The Set LDAP UserBaseDN command is used to set the base (DN) for the login username search. This is where the search will start, and will include all subtrees. Maximum size is 100 characters.

To set the user search base DN:

1. At the command prompt, type **`ldap userbasedn`**, and press **Enter**. At the following prompt, type the search base DN and press **Enter**.

Example

The following sets the DN User search base for MSAD to 'cn=Users,dc=lantronixlantronix,dc=com':

```
SLP:  set ldap userbasedn<Enter>
Enter User Search Base DN (Max characters
100):
cn=Users,dc=lantronix,dc=com<Enter>
```

Setting the authentication order:

The Set Authorder command sets the authentication order for remote authentication sessions. The SLP supports two methods for authentication order-Remote-> Local and Remote Only.

The Remote ->Local method first attempts authentication with the Active Directory server and if unsuccessful then with the local user database on the SLP device.

The Remote Only method attempts authentication only with the Active Directory server and if unsuccessful, access is denied.

Note: *With the Remote Only method, if authentication fails due to a communication failure with the Active Directory server, automatic authentication fallback will occur to authenticate with the local user data base on the SLP device.*

To set the authentication order:

1. At the command prompt, type **`ldap authorder`**, followed by **remotelocal** or **remoteonly** and press **Enter**.

Note: *Lantronix recommends NOT setting the authentication order to Remote Only until the LDAP has been fully configured and tested.*

Displaying the LDAP configuration information:

- The Show LDAP command displays LDAP configuration information
- Enabled-disabled status of LDAP support
- Directory Services server IP address and port
- Bind request password type and remote authentication order
- Search bind distinguished name and password
- User search base distinguished name and filter
- Group membership attribute and type

Note: *With the Remote Only method, if authentication fails due to a communication failure with the Active Directory server, automatic authentication fallback will occur to authenticate with the local user data base on the SLP device.*

To display the LDAP configuration information:

1. At the command prompt, type **`show ldap`** and press **Enter**.

Example

The following command displays the LDAP configuration information:

```
SLP:  show ldap
 LDAP Configuration
  LDAP:   Enabled
  Host 1: 98.76.54.32
  Host 2: ldap.lantronix.com
  Port:   8888
  TLS/SSL: Yes
  Bind Type: MD5
  Auth Order: Remote -> Local

Search Bind
  DN: cd=guest,cn=Users,dc=lantronix,dc=com
  Password: OpenSesame
  User Search
  Base DN: cn=Users,dc=lantronix.com
  Filter: (samaccountname=%s)
  Group Membership
  Attribute: memberof
  Value Type: DN
```

Setting the DNS IP address:

The Set DNS command sets the TCP/IP address of the Domain Name server (DNS).

Note: *LDAP requires the definition of at least one Domain Name server.*

To display the DNS configuration information, use the Show Network command as described in Displaying network configuration information on page 60.

To set the DNS IP address:

1. At the command prompt, type **`set`** followed by **dns1** or **dns2** and the Domain Name server's IP address. Press **Enter**.

Example

The following sets the primary Domain Name server IP address to 98.76.54.254:

```
SLP:  set dns1 98.76.54.254<Enter>
```

Verifying the DNS configuration:

The Ping command may be used to verify the configuration of the DNS IP address.

To verify the DNS configuration:

1. At the command prompt, type **`ping`** followed by the domain component of the Directory Services server previously configured and press **Enter.**

Example

The following command verifies the DNS configuration:

```
SLP:  ping lantronix.com
Pinging lantronix.com [98.76.54.32] with 64
bytes of data
Reply from 98.76.54.32: bytes=64 pseq=0
triptime =0
Reply from 98.76.54.32: bytes=64 pseq=1
triptime =0
Reply from 98.76.54.32: bytes=64 pseq=2
triptime =0
Reply from 98.76.54.32: bytes=64 pseq=3
triptime =0
Reply from 98.76.54.32: bytes=64 pseq=4
triptime =0
```

Configuring LDAP Groups

Creating an LDAP group

The Create LDAPGroup command creates an LDAP group.

To create an LDAP group:

1. At the command prompt, type **`create ldapgroup,`** optionally followed by a group name. Press **Enter.**

Example

The following command creates the LDAP group PowerUser:

```
SLP:  create ldapgroup PowerUser<Enter>
```

Removing an LDAP group:

The Remove LDAPGroup command removes an LDAP group.

To remove an LDAP group:

1. At the command prompt, type **`remove ldapgroup,`** optionally followed by a group name. Press **Enter.**

Setting the LDAP group access level privileges

The set LDAPGroup Access command sets the access level privileges for an LDAP group. The SLP has four defined access privilege levels; Admin, User, On-Only and

View—Only. For more information on user access levels, see *Changing a user's access privilege level*: on page 17.

To set the access level privilege for an LDAP group:

1. At the command prompt, type **`set ldapgroup access,`** followed by **admin, user, ononly** or **viewonly**, optionally followed by a LDAP a group name. Press **Enter.**

Examples

The following command sets the LDAP group access level for LDAPAdmin to Admin:

```
SLP:  create ldapgroup access admin
ldapadmin<Enter>
```

The following command sets the LDAP group access level for PowerUser to User:

```
SLP:  create ldapgroup access user
poweruser<Enter>
```

Granting and removing input status viewing privileges

The set LDAPGroup Envmon command grants or removes input status viewing privileges to/from an LDAP group.

To grant or remove input status viewing privileges for an LDAP group:

1. At the command prompt, type **`set ldapgroup envmon,`** followed by **on** or **off,** optionally followed by a group name and press **Enter.**

Example

The following command grants input status viewing privileges to the LDAP group PowerUser:

```
SLP:  set ldapgroup envmon on
poweruser<Enter>
```

Displaying the LDAP access privilege levels

The List LDAPGroups command displays all defined LDAP groups with their access privilege level.

To display LDAP group access privilege levels:

1. At the command prompt, type **`list ldapgroups`** and press **Enter.**

Example

The following command displays all LDAP groups with their access privilege level:

```
SLP:  list ldapgroups<Enter>
LDAP          Access              Environmental
Group Name    Level               Monitoring

LDAPAdmin     Admin               Allowed
PowerUser     User                Allowed
User          On-Only             Not Allowed
Guest         View-Only           Not Allowed
```

Adding outlet access to an LDAP group

The Add OutletToLDAP command grants an LDAP group access to one or all outlets. To grant access for more than one outlet, but not all outlets, you must use multiple Add OutletToLDAP commands.

To grant outlet access to an LDAP group:

1. At the command prompt, type **`add outlettoldap,`** optionally followed by an outlet name and a group name**.** Press **Enter** or type **`add outlettoldap all`**, followed by a group name and press **Enter.**

Examples

The following commands grant the LDAP group PowerUser access to outlets A1 and Webserv_1:

```
SLP: add outlettoldap .a1 poweruser<Enter>
SLP: add outlettoldap WebServer_1
poweruser<Enter>
```

Deleting outlet access for an LDAP group

The Delete OutletFromLDAP command removes an LDAP group's access to one or all outlets. You cannot remove access to any outlet for an administrative level group.

To delete outlet access for an LDAP group:

2. At the command prompt, type **`delete outletfromldap,`** optionally followed by an outlet name and a group name**.** Press **Enter** or type **`delete outlettoldap all`**, followed by a group name and press **Enter.**

Adding outlet group access to an LDAP group

The Add GroupToLDAP command grants an LDAP group's access to an outlet group. To grant access for more than one outlet group, you must use multiple Add GroupToLDAP commands.

To grant outlet group access to an LDAP group:

3. At the command prompt, type **`add grouptoldap,`** optionally followed by an outlet group name. Press **Enter.**

Examples

The following commands grant LDAP group access to the outlet groups serverGroup_1 and ServerGroup_2:

```
SLP: add grouptoldap servergroup_1
poweruser<Enter>
SLP: add grouptoldap servergroup_2
poweruser<Enter>
```

Deleting outlet group access for an LDAP group

The Delete GroupFromLDAP command removes an LDAP group's access to an outlet group. You cannot remove access to any group for an administrative level group.

To delete outlet group access for an LDAP group:

1. At the command prompt, type **`delete groupfromldap,`** optionally followed by an outlet name and an LDAP group name**.** Press **Enter.**

Adding serial port access for an LDAP group

The Add PortToLDAP command grants an LDAP group access to the serial port.

To grant serial port access to an LDAP group:

1. At the command prompt, type **`add porttoldap console`** and a group name. Press **Enter.**

Deleting serial port access for an LDAP group

The Delete PortFromLDAP command removes an LDAP group's access to the serial port. You cannot remove access to the serial port for an administrative level group.

To delete serial port access for an LDAP group:

1. At the command prompt, type **`delete portfromldap console`** and a group name. Press **Enter.**

Displaying LDAP Group access

The List LDAPGroup command displays all access rights for an LDAP group.

To display LDAP Group access:

At the command prompt, type **`list ldapgroup`, optionally followed by a** group name. Press **Enter.**

Example

The following command displays information about the LDAP group PowerUser:

```
SLP: list ldapgroup poweruser<Enter>
  Username: PowerUser
    Outlet    Outlet
    ID        Name
   .A1       DataServer_1
   .A2       WebServer_1
  Groups:
    ServerGroup_1
    ServerGroup_2
    More [Y/es N/o]: Y
  Ports:
    Port       Port
    ID         Name
    Console    Console
```

TACACS+

The SLP family of products supports the Terminal Access Controller Access Control System (TACACS+) protocol. This enables authentication and authorization with a central TACACS+ server; user accounts do not need to be individually created locally on each SLP device.

This allows administrators to pre-define and configure (in each SLP product, and in the TACACS+ server) a set of necessary TACACS+ privilege levels, and users access rights for each. User's access rights can then be assigned or revoked simply by making the user a member of one-or-more pre-defined SLP TACACS+ privilege levels. User account rights can be added, deleted, or changed within TACACS+ without any changes needed on individual SLP products.

The SLP supports 16 different TACACS+ privilege levels; 15 are entirely configurable by the system administrator (1 is reserved for default Admin level access to all SLP resources).

TACACS+ Command Summary

Command	Description
Set Authorder	Specifies the authentication order for each new session attempt
Set TACACS	Enables/disables SSL support
Set TACACS Host	Sets the IP address or hostname of the TACACS server
Set TACACS Key	Sets the TACACS encryption key
Set TACACS Port	Sets the TACACS server port number
Show TACACS	Displays TACACS configurations
Add GrouptoTACACS	Grants a TACACS account access to one or more groups
Add OutlettoTACACS	Grants a TACACS account access to one or all outlets
Add PorttoTACACS	Grants a TACACS account access to one or serial ports
Delete GroupfromTACACS	Removes access to one or more groups for a TACACS account
Delete OutlettoTACACS	Removes access to one or more outlets for a TACACS account
Delete PortfromTACACS	Removes access to one or more serial ports for a TACACS account
Set TacPriv Access	Sets the access level for a TACACS account
Set TacPriv Envmon	Grants or removes privileges to view input and environmental monitoring status
List TacPrivs	Displays access levels for all TACACS accounts
List TacPriv	Displays all accessible outlet/groups/ports for a TACACS account

Enabling and Setting up TACACS+ Support

There are a few configuration requirements for properly enabling and setting up TACACS+ support. Below is an overview of the minimum requirements:

1. Enable TACACS+ support.
2. Define the IP address and domain component of at least one TACACS+server.
3. Set the TACACS+ key configured on the supporting TACACS+server.

Enabling and disabling TACACS+ support:

The Set TACACS command is used to enable or disable TACACS+ support.

To enable or disable TACACS+ support:

At the SLP: prompt, type **set tacacs**, followed by **enabled** or **disabled** and press **Enter**.

Setting the TACACS+ server address:

The Set TACACS Host command sets the IP address or hostname of the TACACS+ server.

To set the TACACS+ server address:

At the SLP: prompt, type **set tacacs**, followed by **host1** or **host2** and the TACACS+ server's IP address or hostname. Press **Enter**.

Examples

The following command sets the primary TACACS+ server address to 98.76.54.32:

```
SLP: set tacacs host1 98.76.54.32<Enter>
```

The following command sets the secondary TACACS+ server address to tacacs.lantronix.com:

```
SLP: set tacacs host2 tacacs.lantronix.com<Enter>
```

Setting the TACACS+ encryption key:

The Set TACACS Key command sets the encryption key used to encrypt all data packets between the SLP and the TACACS+ server. This key must match the key configured on the TACACS+ server.

To set the encryption key:

At the SLP: prompt, type **set tacacs key** and press **Enter**.

At the TACACS+ Key: prompt, type an encryption key of up to 60 alphanumeric and other typeable characters - (ASCII 33 to 126 decimal) are allowed; encryption keys are case sensitive. Press **Enter**. To specify no password, press **Enter**.

At the Verify TACACS+ Key: prompt, retype the key. Press **Enter**. To verify no password, press **Enter** at the prompt.

Example

```
SLP: set tacacs key<Enter>
   TACACS+ Key: <Enter>
   Verify TACACS+ Key: <Enter>
```

For security, key characters are not displayed.

Note: *A key size of zero results in no encryption being applied which may not be supported by the TACACS+ server and is not recommended for a production environment.*

Changing the TACACS port:

With TACACS support enabled, the SLP sends TACACS requests to the default TACACS port number 49. This port number may be changed using the Set TACACS Port command.

To change the TACACS port:

At the SLP: prompt, type **set tacacs port**, followed by the port number and press **Enter**.

Example

The following changes the TACACS port number to 50:

```
SLP: set tacacs port 50<Enter>
```

Setting the authentication order:

The Set Authorder command sets the authentication order for remote authentication sessions. The SLP supports two methods for authentication order - Remote -> Local and Remote Only.

The Remote -> Local method first attempts authentication with the TACACS+ server and if unsuccessful with the local user database on the SLP device.

The Remote Only method attempts authentication only with the TACACS+ server and if unsuccessful, access is denied.

Note: *With the Remote Only method, if authentication fails due to a communication failure with the TACACS+ server automatic authentication fallback will occur to authenticate with the local user data base on the SLP device.*

To set the authentication order:

At the SLP: prompt, type **set authorder**, followed by **remotelocal** or **remoteonly** and press **Enter**.

Note: *Lantronix recommends NOT setting the authentication order to Remote Only until the TACACS+ has been fully configured and tested.*

Displaying TACACS+ configuration information:

The Show TACACS command displays TACACS+ configuration information.

To display the TACACS configuration information:

At the SLP: prompt, type **show tacacs** and press **Enter**.

Example

The following command displays the TACACS configuration information:

```
SLP: show tacacs<Enter>

   TACACS+ Configuration

      TACACS+:        Enabled

      Host 1:         98.76.54.32
      Host 2:         tacacs.lantronix.com

      Port:           50

      TACACS+ Key:    (Set)

      Auth Order:     Remote->Local
```

Configuring TACACS+ Privilege Levels

Setting TACACS+ account access level privileges:

The Set TacPriv Access command sets the access level privileges for a TACACS+ account. The SLP has four defined access privilege levels; Admin, User, On-Only and View-Only. For more information on user access levels, see Setting user access level privileges on page 43.

To set the access level privilege for a TACACS+ account :

At the SLP: prompt, type **set tacpriv access**, followed by **admin**, **user**, **ononly** or **viewonly,** optionally followed by a TACACS+ account number and press **Enter**.

Examples

The following command sets the TACACS+ account access level for account 14 to Admin:

```
SLP: set tacpriv access admin 14<Enter>
```

The following command sets the TACACS+ account access level for account 5 to User:

SLP: set tacpriv access user 5<Enter>Granting and removing input status viewing privileges:

Granting and removing input status viewing privileges:

The Set TacPriv Envmon command grants or removes input status viewing privileges to/from a TACACS+ account.

To grant or remove input status viewing privileges for a TACACS+ account:

At the SLP: prompt, type **set tacpriv envmon**, followed by **on** or **off**, optionally followed by a TACACS+ account number and press **Enter**.

Example

The following command grants input status viewing privileges to the TACACS+ account 5:

```
SLP: set tacpriv envmon on 5<Enter>
```

Displaying the TACACS+ access privilege levels:

The List TacPrivs command displays all TACACS+ accounts with their access privilege levels.

To display TACACS+ account access privilege levels:

At the SLP: prompt, type **list tacprivs** and press **Enter**.

Example

The following command displays all TACACS+ account with their access privilege level:

```
SLP: list tacprivs<Enter>

   TACACS              Access        Environmental
   Account Name        Level         Monitoring

   TACAdmin            Admin         Allowed
   PowerUser           User          Allowed
   User                On-Only       Not Allowed
   Guest               View-Only     Not Allowed
```

Adding outlet access to a TACACS+ account:

The Add OutletToTACACS command grants a TACACS+ account access to one or all outlets. To grant access for more than one outlet, but not all outlets, you must use multiple Add OutletToTACACS commands.

To grant outlet access to a TACACS+ account:

At the SLP: prompt, type **add outlettotacacs**, optionally followed by an outlet name and a TACACS+ account number. Press **Enter**, or

Type **add outlettotacacs all**, followed by a TACACS+ account number and press **Enter**.

Examples

The following commands grant a TACACS+ account 5 access to outlets A1 and Webserver_1:

```
SLP:add outlettotacacs .a1 5<Enter>
SLP:add outlettotacacs WebServer_1 5<Enter>
```

Deleting outlet access for a TACACS+ account:

The Delete OutletFromTACACS command removes a TACACS+ account's access to one or all outlets. You cannot remove access to any outlet for an administrative level account.

To delete outlet access for a TACACS+ account:

At the SLP: prompt, type **delete outletfromtacacs**, optionally followed by an outlet name and a TACACS+ account number. Press **Enter**, or

Type **delete outletfromtacacs all**, followed by a TACACS+ account number and press **Enter**.

Adding outlet group access to a TACACS+ account:

The Add GroupToTACACS command grants a TACACS+ account access to an outlet group. To grant access for more than one outlet group, you must use multiple Add GroupToTACACS commands.

To grant outlet group access to a TACACS+ account:

At the SLP: prompt, type **add grouptotacacs**, optionally followed by an outlet group name and a TACACS+ account number. Press **Enter**.

Examples

The following commands grants to a TACACS+ account number 5 access to the outlet groups ServerGroup_1 and ServerGroup_2:

```
SLP:add grouptotacacs servergroup_1 5<Enter>
SLP:add grouptotacacs servergroup_2 5<Enter>
```

Deleting outlet group access for a TACACS+ account:

The Delete GroupFromTACACS command removes a TACACS+ account's access to an outlet group. You cannot remove access to any group for an administrative level account.

To delete outlet group access for a TACACS+ account:

At the SLP: prompt, type **delete groupfromtacacs**, optionally followed by a outlet group name and a TACACS+ account number. Press **Enter**.

Adding serial port access to a TACACS+ account:

The Add PortToTACACS command grants a TACACS+ account access to the serial port.

To grant serial port access to a TACACS+ account:

At the SLP: prompt, type **add porttotacacs console** and a TACACS+ account number. Press **Enter**.

Deleting serial port access for a TACACS+ account:

The Delete PortFromTACACS command removes a TACACS+ account's access to the serial port. You cannot remove access to the serial port for an administrative level account.

To delete serial port access for a TACACS+ account:

At the SLP: prompt, type **delete portfromtacacs console** and a TACACS+ account number. Press **Enter**.

Displaying TACACS account access:

The List TacPriv command displays all access rights for a TACACS+ account.

To display TACACS account access:

At the SLP: prompt, type **list tacpriv**, optionally followed by a TACACS+ account. Press **Enter**.

Example

The following command displays information about the TACACS+ account 1:

```
SLP: list tacpriv 1<Enter>

   TACACS+ Privilege Level: 1

      Outlet   Outlet
      ID       Name

      .A1      DataServer_1
      .A2      WebServer_1

      Groups:

         ServerGroup_1
         ServerGroup_2

   More (Y/es N/o): Y

Ports:

         Port ID   Port Name

         Console   Console
```

Members of the TACACS privilege level 1 account may access the following outlets, outlet groups and serial ports: outlet A1 which has a descriptive name of DataServer_1, outlet A2 which has a descriptive name of WebServer_1, group ServerGroup_1 group ServerGroup_2 and Console serial port.

TACACS+ Technical Specifications

Authentication START Packet includes:

action = 1 (TAC_PLUS_AUTHEN_LOGIN)
priv_lvl = 0 (TAC_PLUS_PRIV_LVL_MIN)
authen_type = 1 (TAC_PLUS_AUTHEN_TYPE_ASCII)
service = 1 (TAC_PLUS_AUTHEN_SVC_LOGIN)
user = (entered username)
port = (access path into the SLP)
rem_addr = 'SLP3_xxxxxx' (xxxxxx is last six digits of MAC address)
data = '' (null)

Note: The password is sent in a CONTINUE packet.

Authorization REQUEST Packet includes:

authen_method = 6 (TAC_PLUS_AUTHEN_METH_TACACSPLUS)
priv_lvl = 0 (TAC_PLUS_PRIV_LVL_MIN)
authen_type = 1 (TAC_PLUS_AUTHEN_TYPE_ASCII)
authen_service = 1 (TAC_PLUS_AUTHEN_SVC_LOGIN)
user = (entered username)
port = (access path into the SLP)
rem_addr = 'SLP3_*xxxxxx*' (xxxxxx is last six digits of Ethernet MAC address)
service = 'shell' (for exec)
cmd = '' (null)

Note: *The access paths into the SLP which support TACACS+ are 'Console', 'Telnet', 'SSH', 'HTTP' and 'HTTPS'. In the case of 'Console' and 'Modem', an administrator is allowed to rename these ports in which case the assigned name is used.*

Logging

The SLP family of products supports logging of system events both internally and externally. An internal log of more than 4000 events is automatically maintained and is reviewable by administrative users. For permanent/long-term log storage, SLP supports the Syslog protocol. And for immediate notification, SLP supports Email notifications.

Log entries include a sequential entry number, a date/time stamp and an event message. The event message is preceded with a message 'type' heading and if the event is tied to a user, the username will be included.

Note: *For date/time stamp support, SNTP server support must be configured. For information on SNTP Administration, see page 59.*

The SLP supports the following event message headers:

- AUTH: All authentication attempts.
- POWER: All power state change requests.
- CONFIG: All system configuration changes.
- EVENT: All general system events. Example: over/under threshold event.

Internal System Log

The internal system log is stored in the local memory and has support for up to 4097 continuously aging entries. The internal system log is only available to administrative users. For instructions on reviewing the internal log, see *View Log* page *32*.

Syslog

The SLP's Syslog support is RFC3164-compliant and enables off-SLP viewing and storage of log messages. The SLP supports external logging to up to two Syslog servers.

Syslog Command Summary

Command	Description
Set Syslog HostIP	Sets the IP address of the Syslog server
Set Syslog Port	Sets the Syslog server port number
Show Syslog	Displays all Syslog configuration information

Setting the Syslog server IP address:

The Set Syslog HostIP command sets the TCP/IP address of the Syslog server.

To set the Syslog server IP address:

At the SLP: prompt, type **set syslog**, followed by **hostip1** or **hostip2** and the Syslog server's IP address. Press **Enter**.

Example

The following command sets the primary Syslog server IP address to 56.47.38.29:

```
SLP: set syslog hostip1 56.47.38.29<Enter>
```

Changing the Syslog server port:

With Syslog support enabled, the Syslog server watches and responds to requests on the default Syslog port number 514. This port number may be changed using the Set Syslog Port command.

To change the Syslog port:

At the SLP: prompt, type **set syslog port**, followed by the port number and press **Enter**.

Example

The following changes the Syslog port number to 411:

```
SLP: set syslog port 411<Enter>
```

Displaying Syslog configuration information:

The Show Syslog command displays Syslog configuration information.

To display the Syslog configuration information:

At the SLP: prompt, type **show syslog** and press **Enter**.

Example

The following command displays the Syslog configuration information:

```
SLP: show syslog<Enter>

   SYSLOG Configuration

      Primary Syslog Server IP Address:      56.47.38.29
      Secondary Syslog Server IP Address:    0.0.0.0
      Syslog Server Port:                    411
```

Email

Email Command Summary

Command	Description
Set Email	Enables or disables Email notification support
Set Email SMTP Host	Sets the SMTP Host IP address or hostname
Set Email SMTP Port	Sets the SMTP server port number
Set Email From	Sets the email 'From' address
Set Email PrimaryTo	Sets the primary recipient email address
Set Email SecondaryTo	Sets the secondary recipient email address
Set Email Event	Enables or disables notification of general system events
Set Email Auth	Enables or disables notification of all authentication attempts
Set Email Power	Enables or disables notification of power state change requests
Set Email Config	Enables or disables notification of configuration changes
Show Email	Displays all Email configuration information

Enabling or disabling Email notification Support:

The Set Email command enables or disables Email notification support.

To enable or disable Email notification support:

At the SLP: prompt, type **set email**, followed by **enabled** or **disabled** and press **Enter**.

Setting the SMTP server address:

The Set Email Host command sets the IP address or hostname of the SMTP server.

To set the SMTP server address:

At the SLP: prompt, type **set email smtp host**, followed by the SMTP server's IP address or hostname and press **Enter**.

Examples

The following command sets the SMTP server address to 55.55.55.55:

```
SLP: set email smtp 55.55.55.55<Enter>
```

The following command sets the SMTP server address to email.lantronix.com:

```
SLP: set email smtp email.lantronix.com<Enter>
```

Changing the SMTP server port:

With SMTP support enabled, the SLP sends SMTP requests to the default SMTP port number 25. This port number may be changed using the Set Email SMTP Port command.

To change the TACACS port:

At the SLP: prompt, type **set email smtp port**, followed by the port number and press **Enter**.

Example

The following changes the SMTP port number to 5555:

```
SLP: set email smtp port 5555<Enter>
```

Setting the 'From' email address:

The Set Email From command sets the 'from' email address. By default, this is set to 'SLP3_' plus the last three octets of the unit's MAC address. Example: 'SLP3_510c90@'

To set the 'From' email address:

At the SLP: prompt, type set email from, followed by the originating email address and press Enter.

Example

The following command sets the 'from' email address to Rack14CDU1@lantronix.com:

```
SLP: set email from Rack14CDU1@lantronix.com<Enter>
```

Setting the 'To' email address:

The Set Email PrimaryTo and Set Email SecondaryTo commands set the recipient email addresses.

To set the 'To' email address:

At the SLP: prompt, type **set email**, followed by **primaryto** or **secondaryto** and the destination email address. Press **Enter**.

Examples

The following command sets the primary 'to' email address to DayAdmin@lantronix.com:

```
SLP: set email primaryto DayAdmin@lantronix.com<Enter>
```

The following command sets the secondary 'to' email address to NiteAdmin@lantronix.com:

```
SLP: set email secondaryto NiteAdmin@lantronix.com<Enter>
```

Enabling or disabling event notification types:

The Set Email Event, Set Email Auth, Set Email Power and Set Email Config commands enable or disable email notification of the event types as described on page 95.

To enable or disable event notification types:

At the SLP: prompt, type **set email**, followed by **event**, **auth**, **power** or **config** and **enabled** or **disabled**. Press **Enter**.

Examples

The following command sets the enables email notification general system events:

```
SLP: set email event enabled<Enter>
```

The following command sets the disables email notification authentications attempts:

```
SLP: set email auth disable<Enter>
```

Displaying Email configuration information:

The Show Email command displays Email configuration information.

To display the Email configuration information:

At the SLP: prompt, type **show email** and press **Enter**.

Example

The following command displays the Email configuration information:

```
SLP: show email

   Email Configuration

      Email Notifications:          Enabled

      SMTP Host:                    email.lantronix.com
      SMTP Port:                    5555

      'From' Address:               Rack14CDU1@lantronix.com
      Primary 'Send To' Address:    DayAdmin@lantronix.com
      Secondary 'Send To' Address:  NiteAdmin@lantronix.com

      Include EVENT Messages:       Enabled
      Include AUTH Messages:        Disabled
      Include POWER Messages:       Disabled
      Include CONFIG Messages:      Disabled
```

5: Troubleshooting and Technical Support

Technical Support

If you are experiencing an error that is not described in this user guide, or if you are unable to fix the error, you may:

Check our online knowledge base at www.lantronix.com/support.

Contact Technical Support in the US:

Phone: 800-422-7044 (US only) or 949-453-7198

Fax: 949-450-7226

Our phone lines are open from 6:00AM - 5:00 PM Pacific Time Monday through Friday, excluding holidays.

Contact Technical Support in Europe, Middle East, and Africa:

Phone: +49 (0) 89 31787 817

E-mail: eu_techsupp@lantronix.com

Firmware downloads, FAQs, and the most up-to-date documentation are available at: www.lantronix.com/support .

When you report a problem, please provide the following information:

Your name, and your company name, address, and phone number

Lantronix model number

Lantronix serial number

Software version

Description of the problem

Debug report (stack dump), if applicable

Status of the unit when the problem occurred (please try to include information on user and network activity at the time of the problem)

A: Resetting to Factory Defaults

You may reset the non-volatile RAM that stores all configurable options. This clears all administrator-editable fields and resets all command line configurable options to their default values, including all user accounts.

You may reset the unit to factory defaults from the command line or the web browser interface, or by pressing the reset button. You must have administrator-level privileges to issue the command. Using the reset button may be necessary when a forgotten password prevents administrator login. Each of the methods updates the current working configuration to the factory defaults.

Note: *Resetting the unit resets all TCP/IP and Telnet/Web configurations. Reconfiguring the TCP/IP and Telnet/web settings will be required*.

To reset to factory defaults from the web browser interface

1. On the **Restart** page in the Tools section of the web browser interface, select Restart and reset to factory defaults from the drop-down menu and press **Apply**.

To reset to factory defaults from the command line

1. At the command prompt, type `restart factory` and press **Enter**.

To reset to factory defaults using the reset button

1. Locate the recessed reset button directly beside the Serial & Ethernet ports. You will need a non-conductive, non-metallic tool that fits inside the recess.
2. Insert the tool in the recess, then depress and hold the reset button for at least ten seconds.

Note: *If the reset button is depressed and held for more than 15 seconds, the reset will abort*.

B: Uploading Firmware

You may upload new versions of firmware using File Transfer Protocol (FTP). This allows access to new firmware releases for firmware improvements and new features additions.

Note: *To begin an FTP upload session, you must first configure the FTP Host address, username/password, filename and file path. For information on configuring the FTP settings required for firmware upload see* 3:*Operations*.

You may initiate an FTP upload session by issuing a command or from the web browser interface. You must have administrator-level privileges to initiate an upload.

To initiate an FTP upload session from the web browser interface

1. On the **Restart** page in the Tools section of the web browser interface, select Restart and upload firmware via FTP from the drop-down menu and press **Apply**.
2. Upon issuing this command the unit will restart and upload the firmware file specified with the FTP Filename command from the previously configured FTP Host. See *FTP Administration* on page 62 for more information.

To initiate an FTP upload session from the command line

The Restart FTPLoad command initiates an upload of firmware. Upon issuing this command the unit will restart and upload the firmware file specified with the FTP Filename command from the previously configured FTP Host. See *FTP Administration* on page 62 for more information.

To initiate an FTP firmware upload session:

1. At the command prompt, type `restart ftpload` and press **Enter**.

C: Technical Specifications

Models

Table C-5-1. Vertical Installation

Model	Voltage	Inlet	Outlets
SLPV1611E-02	100-120V, 50/60Hz	IEC 60320/C20	16 - NEMA 5-20R
SLPV1612E-02	208-230V, 50/60Hz	IEC 60320/C20	16 - IEC 60320/C13
SLPV1614G-02*	208-230, 50/60Hz	NEMA L6-30P, 30A locking	16 - IEC 60320/C13

Table C-5-2. Vertical Expansion Unit

Model	Voltage	Inlet	Outlets
SLPY1611E-02**	100-120V, 50/60Hz	IEC 60320/C20	16 - NEMA 5-20R
SLPY1612E-02**	208-230V, 50/60Hz	IEC 60320/C20	16 - IEC 60320/C13

Table C-5-3. Horizontal/Rack Installation

Model	Voltage	Inlet	Outlets
SLPH0811E-02	100-120V, 50/60Hz	IEC 60320/C20	8 - NEMA 5-20R
SLPH0812E-02	208-230V, 50/60Hz	IEC 60320/C20	8 - IEC 60320/C13
SLPH0814G-02*	208-230V,50/60Hz	NEMA L6-30P,30A locking	8 - IEC 60320/C13

Table C-5-4. Horizontal/Rack Expansion Unit

Model	Voltage	Inlet	Outlets
SLPX0811E-02	100-120V, 50/60Hz	IEC 60320/C20	8 - NEMA 5-20R
SLPX0812E-02	208-230V, 50/60Hz	IEC 60320/C20	8 - IEC 60320/C13

Table C-5-5. Power Ratings

Model	Input Current Ratings[1]		Output Current Ratings	
	Voltage	Current	Outlet	Total
SLPH08x1E-02	100-120V 50/60 Hz	16	16	16
*SLPX08x1E-02				
SLPV16x1E-02				
*SLPY16x1E-02				
SLPH08x2E-02	208-230V	16	12	16

SLPX08x2E-02	50/60 Hz			
*SLPV16x2E-02				
*SLPY16x2E-02				
SLPH0814G-02	208-230V 50/60 Hz	24	12	24
SLPV1614G-02				

[1] Current ratings are in amperes.
***Expansion model**

Table C-5-6. Physical Specifications

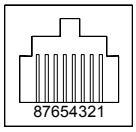
		SLP-V16xxx-02	SLP-H08xxx-02
Physical	Size	65.0 x 1.75 x 2.25 in.	1.75 x 17.0 x 7.0 in.
	Weight	13.2 lbs	8.2 lbs
Temperature	Operating	0° to 50° C (32° to 122° F)	
	Storage	-40° to 85° C (-40° to 185° F)	
Relative Humidity	Operating	10 to 90%, non-condensing	
	Storage	10 to 90%, non-condensing	
Approvals		FCC Class A, Part 15 cTUVus (US & Canada) to UL 60950:2003 and CAN/CSA 22.2 No 60950-1-03 European Union (TUVGS mark) EN60950-1:2001	

Data Connections

RS-232 port

All units are equipped standard with an RJ45 DTE RS-232c serial port. This connector may be used for direct local access or from other serial devices such as a terminal server. An RJ45 serial rollover cable is provided for connection to an RJ45 DTE serial port.

Table C-5-7. RS-232 Port

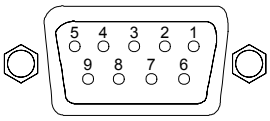


Pin	DTE Signal Name		Input/Output
1	Request to Send	RTS	Output
2	Data Terminal Ready	DTR	Output
3	Transmit Data	TD	Output
4	Signal Ground		
5	Signal Ground		
6	Receive Data	RD	Input
7	Data Set Ready	DSR	Input
8	Clear to Send	CTS	Input

RJ45 to DB9F serial port adapter

An RJ45 to DB9F serial port adapter is provided for use in conjunction with the RJ45 serial rollover cable to connect to a PC DB9M DTE serial port. The adapter pinouts below reflect use of the adapter with the provided RJ45 serial rollover cable.

Table C-5-8. RJ45 to DB9 Serial Port Adapter



Pin	DCE Signal Name		Input/Output
1			
2	Receive Data	RD	Output
3	Transmit Data	TD	Input
4	Data Terminal Ready	DTR	Input
5	Signal Ground		
6	Data Set Ready	DSR	Output
7	Request to Send	RTS	Input
8	Clear to Send	CTS	Output

Ethernet LED Indicators

Table C-5-9. LED Description

LED	Color	Description
Network Link	Yellow (lower)	Network Link is operational. On (continuously) indicates that an Ethernet connection is made.
Network Activity	Green (upper)	Network Activity: on when network traffic detected, off when no network traffic detected.
		Diagnostics: flashes three times in even duration during power up or reset, indicating a successful startup.

Outlet LED Indicators

Units are equipped with a status LED for each power receptacle. A lit/on LED indicates that power is being supplied at the port and a darkened/off LED indicates that there is no power at the port.

Temperature/Humidity Probe (Accessory)

The SecureLinx SLP Temperature and Humidity Probe monitors data center environmental conditions to ensure they do not exceed recommended thresholds. The temperature and humidity probe is a combination probe that supports both temperature and humidity and plugs into either T/H1 or T/H2.

Lantronix Part Number	Description
SLPM1TH10-01	Probe: Temperature and Humidity, 10 Ft. cable

Table C-5-10. Temperature/Humidity Probe Technical Specifications

Category	Description
Temperature	Operating: -40 – 120 °C. At normal operating range (0-50°C), accuracy is ± 1 degree.
Relative humidity	Non-condensing: 0-95% relative humidity. At normal operating range (20-80% relative humidity) accuracy is ± 3%.

D: Compliance Information

(according to ISO/IEC Guide 22 and EN 45014)

Manufacturer's Name & Address:
Lantronix 15353 Barranca Parkway, Irvine, CA 92618 USA

Declares that the following product:

Product Name Model: SecureLinx SLP Remote Power Manager

Conforms to the following standards or other normative documents:

USA and Canada

FCC Class A, Part 15

cTUVus (US & Canada) to UL 60950:2003 and CAN/CSA 22.2 No 60950-1-03

European Union

(TUVGS mark) EN60950-1:2001

Manufacturer's Contact:
Director of Quality Assurance, Lantronix
15353 Barranca Parkway, Irvine, CA 92618 USA
Tel: 949-453-3990
Fax: 949-453-3995

RoHS Notice:

All Lantronix products in the following families are China RoHS-compliant and free of the following hazardous substances and elements:

- Lead (Pb)
- Cadmium (Cd)
- Mercury (Hg)
- Hexavalent Chromium (Cr (VI))
- Polybrominated biphenyls (PBB)
- Polybrominated diphenyl ethers (PBDE)

Product Family Name	Toxic or hazardous Substances and Elements					
	Lead (Pb)	Mercury (Hg)	Cadmium (Cd)	Hexavalent Chromium (Cr (VI))	Polybrominated biphenyls (PBB)	Polybrominated diphenyl ethers (PBDE)
UDS1100 and 2100	0	0	0	0	0	0
EDS	0	0	0	0	0	0
MSS100	0	0	0	0	0	0
IntelliBox	0	0	0	0	0	0
XPress DR & XPress-DR+	0	0	0	0	0	0
SecureBox 1101 & 2101	0	0	0	0	0	0
WiBox	0	0	0	0	0	0
UBox	0	0	0	0	0	0
MatchPort	0	0	0	0	0	0
SLC	0	0	0	0	0	0
XPort	0	0	0	0	0	0
WiPort	0	0	0	0	0	0
SLB	0	0	0	0	0	0
SLP	0	0	0	0	0	0
SCS	0	0	0	0	0	0
SLS	0	0	0	0	0	0
DSC	0	0	0	0	0	0

O: toxic or hazardous substance contained in all of the homogeneous materials for this part is below the limit requirement in SJ/T11363-2006.
X: toxic or hazardous substance contained in at least one of the homogeneous materials used for this part is above the limit requirement in SJ/T11363-2006.

Warranty

Lantronix warrants each Lantronix product to be free from defects in material and workmanship for a period of **TWO YEARS** after the date of shipment. During this period, if a customer is unable to resolve a product problem with Lantronix Technical Support, a Return Material Authorization (RMA) will be issued. Following receipt of an RMA number, the customer shall return the product to Lantronix, freight prepaid. Upon verification of warranty, Lantronix will -- at its option -- repair or replace the product and return it to the customer freight prepaid. If the product is not under warranty, the customer may have Lantronix repair the unit on a fee basis or return it. No services are handled at the customer's site under this warranty. This warranty is voided if the customer uses the product in an unauthorized or improper way, or in an environment for which it was not designed.

Lantronix warrants the media containing its software product to be free from defects and warrants that the software will operate substantially according to Lantronix specifications for a period of **60 DAYS** after the date of shipment. The customer will ship defective media to Lantronix. Lantronix will ship the replacement media to the customer.

* * * *

In no event will Lantronix be responsible to the user in contract, in tort (including negligence), strict liability or otherwise for any special, indirect, incidental or consequential damage or loss of equipment, plant or power system, cost of capital, loss of profits or revenues, cost of replacement power, additional expenses in the use of existing software, hardware, equipment or facilities, or claims against the user by its employees or customers resulting from the use of the information, recommendations, descriptions and safety notations supplied by Lantronix. Lantronix liability is limited (at its election) to:

refund of buyer's purchase price for such affected products (without interest)

repair or replacement of such products, provided that the buyer follows the above procedures.

There are no understandings, agreements, representations or warranties, express or implied, including warranties of merchantability or fitness for a particular purpose, other than those specifically set out above or by any existing contract between the parties. Any such contract states the entire obligation of Lantronix. The contents of this document shall not become part of or modify any prior or existing agreement, commitment or relationship.

For details on the Lantronix warranty replacement policy, go to our web site at www.lantronix.com/support/warranty .